Juho Erkkilä

Pääsynhallintamenetelmät ja niiden tehostaminen IT-ulkoistuspalveluntarjoajan näkökulmasta

Sähkötekniikan korkeakoulu

Diplomityö, joka on jätetty opinnäytteenä tarkastettavaksi diplomi-insinöörin tutkintoa varten Espoossa 23.5.2012.

Työn valvoja:

Dos. Kalevi Kilkki

Työn ohjaaja:

DI Arsi Heinonen

Aalto-yliopisto
Sähkötekniikan korkeakoulu

AALTO-YLIOPISTO
SÄHKÖTEKNIIKAN KORKEAKOULU

DIPLOMITYÖN
TIIVISTELMÄ

Tekijä: Juho Erkkilä

Työn nimi: Pääsynhallintamenetelmät ja niiden tehostaminen IT-ulkoistuspalveluntarjoajan näkökulmasta

Päivämäärä: 23.5.2012 Kieli: Suomi Sivumäärä:10+69

Tietoliikenne- ja tietoverkkotekniikan laitos

Professuuri: Tietoverkkotalous Koodi: ETA3003

Valvoja: Dos. Kalevi Kilkki

Ohjaaja: DI Arsi Heinonen

Diplomityössä esitellään pääsynhallinta osana IT palvelutoimintaa, tutustutaan erilaisiin pääsynhallintamenetelmiin, ja pohditaan miten pääsynhallintaa voitaisiin tehostaa IT ulkoistuspalveluntarjoajan näkökulmasta. Pääsynhallintamenetelmät luottavat olemassa oleviin tietoturvan- ja identiteetinhallintamenetelmiin pyrkien toteuttamaan sovittua tietoturvapolitiikkaa.

Työssä esitellään tapaustutkimuksena miten pääsynhallinta on määritelty palveluna IT-ulkoistuspalveluita tarjoavassa yrityksessä ja millaisin menetelmin pääsynhallintaa yrityksessä toteutetaan. Tapaustutkimuksen tulokset osoittavat, että pääsynhallinta on puutteellisesti toteutettu, johtuen osittain siitä, ettei pääsynhallintaa ole määritelty yrityksessä palvelutoiminnoksi.

Pääsynhallinnan parantamiselle yrityksessä esitellään toteuttamisehdotus, jonka tarkoituksena on tarjota kattava kokonaiskuva siitä, miten pääsynhallinta voitaisiin IT-ulkoistuspalveluita tarjoavassa yrityksessä toteuttaa. Pääsynhallinta kuvattiin yhdeksi palvelutoiminnoksi siten, että se osaltaan lisäisi yrityksen tietoturvaa ja tehostaisi käyttöoikeuspyyntöjen hallintaa ja toteutusta.

Arvioinnin perusteella toteutusehdotus on yritykselle suositeltava toteuttaa. Se tarjoaa tehokkaaman tavan hallinnoida ja toteuttaa käyttöoikeuspyyntöjä ja lisää osaltaan yrityksen tietoturvaa. RBAC perustainen pääsynhallinta myös mahdollistaa toimintatavan linjaamisen yleisten alan parhaiden käytäntöjen ja standardien kanssa.

Avainsanat: Pääsynhallinta, pääsyn kontrollointi, käyttöoikeuksien hallinta, identiteetinhallinta, IAM, DAC, MAC, RBAC, tietoturvapolitiikka, reference monitor

AALTO UNIVERSITY
SCHOOL OF ELECTRICAL ENGINEERING

ABSTRACT OF THE
MASTER'S THESIS

Author: Juho Erkkilä

Title: Access management methods and enhancement of the methods in IT Outsoursing Service Provider organization

Date: 23.5.2012 Language: Finnish Number of pages:10+69

Department of Communications and Networking

Professorship: Communications Ecosystem Code: ETA3003

Supervisor: Docent Kalevi Kilkki

Instructor: M.Sc. (Tech.) Arsi Heinonen

This master's thesis introduces access management as a part of IT service activities, discusses how different access management methods are used in IT Outsoursing Service Provider organization, and how those could be enhanced. Access management methods relies on information security management and identity management, which provide essential policies and methods required for performing access management.

A case study was performed to IT Outsoursing Service Provider organization to study how the access management is defined as a service and with what kind of methods and tools access management is carried out within the organization. Gathered results from the case study reveal that current way of performing access management within the organization is deficient partly because it has not been recoqnized as a service activity.

To enhance the access management within the organization, an implementation proposal was constructed. Proposal provides a comprehensive overview how access management could be defined and implemented within the organization. Access management was defined as a service in a way that it would increase organizations information security and improve the management and realization of the access requests.

Based on the evaluation, the implementation proposal is recommended for the organization. It increases the efficiency of the management and realization of the access request as well as organization overal information security. By introducing RBAC based access management, proposal enables access management activities to be in line with industry's best practices and standards.

Keywords: Access Management, Access Control, User rights management, Identity Management, IAM, DAC, MAC, RBAC, Information Security Policy, Reference Monitor

Esipuhe

Haluan kiittää Dosentti Kalevi Kilkkiä kärsivällisyydestä työn edistymisessä ja kannustavasta asenteesta työtä kohtaan. Ohjaaja Arsi Heinosta haluan kiittää laaja-alaisesta asiantuntemuksesta ja näkemyksen antamisesta työhön sekä hyvästä ohjauksesta. Kiitos Atos IT Solutions and Services Oy:lle mahdollisuudesta tehdä diplomityö yritykselle. Henkilöt, joiden kanssa olen saanut yrityksessä työskennellä ovat mitä parhaimpia työkavereita ja olen saanut heiltä paljon apua ja tukea niin diplomityön suorittamisessa kuin muissa työtehtävissä. Kiitos teille.

Erityismaininta Niina Järviselle tukemisesta, oikolukemisesta, jaksamisesta ja kannustamisesta työn etenemisen aikana. Kiitos!

Otaniemi, 23.05.2012

Juho Erkkilä

Sisältö

Lyhenteet ja termit

Lyhenteet

ABAC	Attribute Based Access Control, ominaisuusperusteinen pääsynhallinta
ARAP	Access Request Approval Process, Atos IT Solutions and Services Oy:n sisäinen käyttöoikeuksien hakemiseen tarkoitettu sovellus
BLP	Bell-LaPadula -malli
CIR	Check In Request, Atos IT Solutions and Services Oy:n sisäinen käyttöoikeuksien hakemiseen tarkoitettu sovellus
CMDB	Configuration Management Database, konfiguraatiotietokanta, joka sisältää IT infrastruktuurin komponentit ja niiden konfiguraatiotiedot
CMweb	Change Management web console, Atos IT Solutions and Services Oy:n sisäinen muutospyynnöille tarkoitettu konsoli
COBIT	Control Objectives for Information and related Technology, sisältää teollisuuden parhaita käytäntöjä ja viitekehyksiä yleisiin ICT-prosesseihin
DAC	Discretionary Access Control, harkinnanvarainen pääsynhallinta
DSD	Dynamic Separation of Duties, dynaaminen tehtävien eriyttäminen
HR	Human Resources, henkilöstöhallinto, joka vastaa yrityksen erilaisista henkilöstöön liittyvistä käytännön tehtävistä sekä lakisääteisistä asioista
IAM	Identity and Access Management, identiteetin- ja pääsynhallinta
ICT	Information and Communication Technology, tieto- ja viestintätekniikka
ISO	International Organization for Standardization, kansainvälinen standardisoimisjärjestö
IT	Information Technology, tietotekniikka
ITIL	Information Technology Infrastructure Library, kokoelma teollisuuden parhaita käytäntöjä IT-palveluiden hallintaan ja johtamiseen
KPI	Key Performance Indicator, suorituskykyilmaisin, jolla arvioidaan tietyn aktiviteetin toiminnallisuutta
LDAP	Lightweight Directory Access Protocol, hakemistopalveluiden käyttöön tarkoitettu verkkoprotokolla
OLA	Operational Level Agreement, operatiivisen tason sopimus, joka määrittelee sisäisten tukiryhmien väliset riippuvuussuhteet ja osapuolten vastuualueet, mukaanlukien prosessit ja aikataulut
RBAC	Role Based Access Control, rooliperusteinen pääsynhallinta
SLA	Service Level Agreement, palvelutasosopimus on osa palvelusopimusta, jossa määritellään palvelulle tietyt vaatimustasot, kuten palveluaika tai -suorituskyky

SOA	Service Oriented Architecture, palvelukeskeinen arkkitehtuuri on järjestelmien kehityksessä ja ohjelmistotekniikassa käytetty joustava suunnitteluperiaate, jossa järjestelmien toiminnot ja prosessit ovat suunniteltu toimimaan itsenäisesti ja käytettäväksi avoimesti standardoitujen rajapintojen kautta
SoD	Separation of Duties, tehtävien eriyttäminen
SPOC	Single Point of Contact, keskitetty yhteydenottopiste, jonne määritetty viestintä ohjataan
SSD	Static Separation of Duties, staattinen tehtävien eriyttäminen
SSO	Single Sign-On, kertakirjautuminen on menetelmä jolla toteutetaan pääsy useisiin kohdejärjestelmiin käyttäjän yhdellä autentikoinnilla. Kertakirjautumisen tarkoituksena on vähentää toistuvia autentikointeja käytettäessä samaa käyttäjätunnusta käyttäviä palveluita.
TCB	Trusted Computing Base, luotettu tietojenkäsittelypohja, jolla tarkoitetaan tietokonejärjestelmään kuuluvista laitteista muodostuvaa kokonaisuutta, joka yhdessä toteuttaa turvapolitiikan
URI	Uniform Resource Identifier, merkkijono, jolla tunnistetaan identifioitavissa oleva internet-resurssi

Termit

Bottom-up menetelmä	Roolien määrittämisen menetelmä, jossa roolit määritellään olemassa oleviin käyttöoikeustietoihin perustuen
Haavoittuvuus	(engl. Vulnerability) Heikkous tai virhe kohdejärjestelmässä, jota voi hyödyntää yksi tai useampi uhka
Identiteetti	(engl. Identity) Aktiivinen itsenäinen kokonaisuus, joka voi olla fyysinen henkilö, kohdejärjestelmä tai verkkolaite, tai ohjelmallinen, joka suorittaa tiettyjä toimintoja. Henkilön kohdalla identiteetillä tarkoitetaan niitä tietoja, jotka erottavat yksilön ja todentavat hänen asemansa organisaatiossa. Identiteetti on aina yksilöllinen.
Kohdejärjestelmä	(engl. Target system) Kohde tai palvelu, johon voidaan anoa oikeutta
Kontrolli	(engl. Control) Tarkoittaa riskien hallinnan keinoja, sisältäen politiikan, toimintatavat, ohjeistuksen, käytännöt ja organisaation rakenteet, jotka voivat olla hallinnollisia, teknisiä, johdollisia tai oikeudellisia.
Käyttöoikeus/oikeus	(engl. Privilege/Access) Todelliset asetukset, jotka mahdollistavat käyttäjälle palvelun käytön tai pääsyn kohdejärjestelmään. Tyypillisiä pääsyoikeusasetuksia ovat lukeminen, kirjoittaminen, suorittaminen, muuttaminen ja poistaminen.
Neljän silmän periaate	Tietoturvaperiaate, jossa hyväksynnän tulee aina tapahtua kahden henkilön toimesta
Partneri/kolmas osapuoli	(engl. Third party/Partner) Henkilö, organisaatio tai taho, joka tekee yhteistyötä tai osallistuu jollakin tavalla organisaation liiketoimintaan, sen tuottamiseen tai tukemiseen
Politiikka	(engl. Policy) Virallisesti ilmaistu menettelytapa, tarkoitus ja suunta
Profiili	(engl. Profile) Identiteetin digitaalinen esitysmuoto, viitaten usein vain tiettyyn käyttäjään. Profiili voi olla myös esitys tietyn tyyppisestä käyttäjämallista, jolloin profiili voidaan siirtää käyttäjältä toiselle.
Prosessi	(engl. Process) Suoritettavien toimenpiteiden sarja, jotka tuottavat määritellyn lopputuloksen. Prosessissa tapahtumat ja suoritteet toistuvat samankaltaisina jostain määritellystä näkökulmasta tarkasteltuna.
Provisiointi	Käyttöoikeuksien luominen tai välittäminen kohdejärjestelmiin

Pääsynhallinta	(engl. Access Management) Tässä diplomityössä pääsynhallinnalla tarkoitetaan käyttäjien pääsy- ja käyttöoikeuksien hallintaa
Pääsyoikeus/valtuus	(engl. Permission) Palvelun toimintojen ja tietojen taso ja laajuus, joita käyttäjällä on valtuus käyttää
Riskanalyysi	(engl. Risk analysis) Systemaattinen tiedon kerääminen ja tarkastelu, tavoitteena tunnistaa ja arvioida riskien lähteet ja vaikutukset
Riski	(engl. Risk) Tapahtuman todennäköisyyden ja negatiivisen seurauksen yhteisvaikutusta
Rooli	Työtehtävä, johon on kuvattu joukko pääsy- ja käyttöoikeuksia, joita tarvitaan työn suorittamiseen
Service Desk	Yrityksen IT-palveluiden keskitetty yhteydenottopiste (SPOC), jonka tarkoituksena on vastaanottaa käyttäjien ja työntekijöiden tietoteknisiä palvelupyyntöjä ja käynnistää niiden käsittely
SharePoint	Microsoft tiedonhallintaratkaisu, joka tarjoaa mm. keskitetyn ja ryhmätyön mahdollistavan dokumenttien hallinnan yrityksen web-sivustoilla
Tiketöintijärjestelmä	Palveluntuottajan palvelupyyntöjen hallintajärjestelmä
Top-down menetelmä	Roolien määrittämisen menetelmä, jossa roolimääritelmät perustuvat yrityksen organisaatiokaavioihin ja prosessikuvauksiin
Uhka	(engl. Threat) Mahdollinen epätoivottu tapahtuma, joka voi aiheuttaa haittaa yhteen tai useampaan kohdejärjestelmään tai organisaatioon

1 Johdanto

Miksi pääsynhallinta on tärkeää yrityksille? Otetaan esimerkki lentokentästä, jossa fyysinen pääsynhallinta, eli kulunvalvonta, on tärkeä turvallisuustekijä. Lentokentällä ei voida sallia jokaisen pääsevän lentokentän kaikille alueille, vaan pääsy alueille on rajoitettu käyttötarkoitusten ja käyttäjäkunnan mukaan. Pääsyoikeudet perustuvat lentokentän ja siellä toimivien yritysten turvapolitiikkoihin ja sääntöihin, joista poikkeaminen vaarantaisi paitsi yritysten liiketoiminnan, myös koko käyttäjäkunnan turvallisuuden. Samaan tapaan tietojärjestelmien pääsynhallinta on tapa hallita ja turvata liiketoiminnan kannalta tärkeät tietopääomat, -järjestelmät ja niiden käyttäjät.

Organisaatioissa tietojärjestelmien käyttäjäkunta voi olla hyvinkin suuri, tietojärjestelmiä paljon ja käyttöaste korkea. Tämä asettaa omanlaisiaan haasteita pääsynhallinnan suunnitteluun ja toteutukseen: tietoturvan näkökulmasta pääsynhallinnan tulee perustua sääntöihin sekä olla hallittavissa ja auditoitavissa. Organisaation etuja vuorostaan ovat nopea ja tehokas pääsynhallinta sekä kulujen pitäminen mahdollisimman alhaisina. IT-ulkoistuspalveluita tarjoavassa yrityksessä tulee lisäksi ottaa huomioon käyttäjäkunnan ja ylläpidettävien järjestelmien monimuotoisuus ja niissä tapahtuvien muutosten tiheys.

Diplomityö on tehty Atos IT Solutions and Services Oy yritykselle. Diplomityössä esitellään pääsynhallinta osana IT palvelutoimintaa ja tutustutaan erilaisiin pääsynhallintamenetelmiin. Diplomityössä käydään läpi tapaustutkimuksena yrityksen pääsynhallinnan nykytilan toteutus ja siinä käytetyt menetelmät. Lisäksi esitellään toteutusehdotus kustannustehokkaasta ja skaalautuvasta pääsynhallintaratkaisusta, joka soveltuisi ja jolla voitaisiin tehostaa käyttöoikeuksienhallintaa yrityksessä. Osana diplomityötä suunniteltiin ITILv3:n mukainen pääsynhallintaprosessi ja rooliperustaista pääsynhallintaa tukeva roolimäärittely.

1.1 Tausta

Atos IT Solutions and Services Oy on IT-palveluita maailmanlaajuisesti tarjoava yritys, joka keskittyy erityisesti IT-ulkoistuspalveluiden tarjoamiseen. Yrityksen tarjoamat IT-palvelut perustuvat kansainvälisesti tunnettuihin ITIL- ja COBIT -käytäntöihin. Yrityksen koko IT-palvelutoiminnalle on myönnetty ISO 9001 laadunhallinnan-, ISO/IEC 20000 palveluidenhallinnan- ja ISO/IEC 27001 tietoturvahallinnan sertifikaatit, joilla vahvistetaan sitoutumista laatuun ja sen jatkuvaan kehittämiseen. Myös yrityksen sisäiset toimintatavat ja prosessit pyritään kehittämään alan parhaisiin käytäntöihin perustuen.

1.2 Tutkimusongelma

Usein pääsynhallinta tarvitsee toteuttaa käyttäjäkunnalle, jolle voidaan määritellä selkeät roolit ja oikeustasot, ja joka kohdistuu rajattuun määrään erilaisia kohdejärjestelmiä tai palveluita. IT-ulkoistuspalveluita tarjoavassa yrityksessä pääsykohteita ovat paitsi yrityksen sisäiset kohdejärjestelmät ja palvelut myös hallinnoidut asiakasjärjestelmät. Kohdejärjestelmien käyttäjiä voivat olla yrityksen omat sisäiset työntekijät sekä ulkoiset työntekijät, kuten partnerit ja asiakkaan työntekijät. Käyttäjäkunnan monimuotoisuus tekee pääsynhallinnasta erityisen tärkeää tietoturvan näkökulmasta: käyttäjien tunnistamisella ja pääsyn rajaamisella oikealle käyttäjäryhmälle pyritään vähentämään yritykseen ja sen tietoturvaan kohdistuvia uhkia.

Atos IT Solutions and Services Oy:n nykyinen pääsynhallinta on toteutettu kahdella eri työkalulla, joissa molemmissa on omat heikkoutensa. Haettavia oikeuksia ei ole tarkasti jaoteltu työkalujen välille, vaan joitakin oikeuksia voi hakea molemmilla työkaluilla ja joitakin oikeuksia puuttuu kummastakin. Loppukäyttäjät kokevat molemmat työkalut vaikeiksi käyttää, eivätkä erota kumpaa työkalua kuuluisi käyttää. Tämä on johtanut osittain siihen, että joitain oikeuksia haetaan suoraan palvelupyyntöinä tiketöintityökalulla, jolloin kirjanpito jaetuista oikeuksista jää puutteelliseksi. Lisäksi yhtenäinen pääsynhallinnan malli ja käsitteellinen prosessikuvaus puuttuvat.

Käyttöoikeuspyyntöjen läpivientiaika pyyntöjen määrään nähden koetaan yrityksessä korkeaksi. Uusi työntekijä, tai työntekijä jonka työnkuva vaihtuu, joutuu usein odottamaan pääsyoikeuksia, joita hän tarvitsee uuden työnkuvansa suorittamiseen. Tapaustutkimuksella on tarkoitus kartoittaa nykyisen pääsynhallinnan toteutus ja tehokkuus sekä arvioida miten hyvin se vastaa yrityksen liiketoiminnallisiin vaatimuksiin.

Tyypillisesti IT-ulkoistuspalveluita tarjoavan yrityksen tuotantotiimeissä työskentelevillä työntekijöillä on hyvin samanlaiset oikeudet keskenään tiimin sisällä. Rooliperustaisia käyttöoikeuksia ei ole yrityksessä määritelty ja käyttöoikeuksia haetaan käyttäjille yksitellen tarpeen mukaan. Rooliperustainen pääsynhallintamalli mahdollisesti vähentäisi yksittäisten käyttöoikeuspyyntöjen määrää ja lisäisi oikeuksien jaon tehokkuutta ja hallittavuutta.

1.3 Arviointikriteeri

Pääsynhallintamenetelmien, siinä käytettävien työkalujen ja toteutusvaihtoehtojen arvioinnissa käytettiin alla lueteltuja arviointikriteerejä. Kriteereiden avulla voidaan olettamuksiin ja tulkintoihin perustuenkin arvioida ratkaisun sopivuutta ja kannattavuutta IT-ulkoistuspalveluita tarjoavan yrityksen toimintaan ja sen hallinnoimiin IT-ympäristöihin.

- Toteutuskelpoisuus: toteutuksen vaatimat henkilö- ja aikaresurssit sekä inves-

toinnit tulevat olla yrityksen kokoon ja liikevaihtoon nähden kohtuulliset.

- Taloudellinen kannattavuus: ratkaisun tulee tuottaa yritykselle säästöjä ja lisäarvoa verrattaessa olemassa olevaan ratkaisuun.
- Ylläpidettävyys ja käytettävyys: toteutus ei saa olla liian monimutkainen työkalun ylläpitäjälle eikä loppukäyttäjälle
- Turvallisuus: toteutus ei saa häiritä käyttäjien päivittäisiä työtehtäviä tai haitata yrityksen IT-ympäristöjä. Sen tulee noudattaa yrityksen tietoturvakäytäntöjä ja käyttöoikeushallinnan osalta parantaa yrityksen tietoturvapolitiikan toteutumista.
- Skaalautuvuus: toteutuksen tulee ottaa huomioon käyttäjäkunnan ja ylläpidettävien järjestelmien monimuotoisuus ja määrä sekä niissä tapahtuvien muutosten yleisyys.
- Sertifioitavuus: toteutuksen tulee olla linjassa yleisesti hyväksyttyjen alan parhaiden käytäntöjen kanssa.

1.4 Diplomityön rakenne

Tämä diplomityö koostuu kahdeksasta kappaleesta. Ensimmäinen kappale toimii johdantona aiheeseen esitellen aiheen taustan ja aiheeseen liittyvän tutkimusongelman sekä toteutuksen arviointikriteerin. Kappaleet 2, 3, 4 ja 5 käsittelevät tutkimusongelmaan liittyvää teoriaa ja taustatietoa.

Kappaleessa 2 käydään läpi, mitä palvelulla ja palvelunhallinnalla tarkoitetaan ja mikä merkitys sillä on IT palveluorganisaatiossa. Lisäksi keskustellaan toimintaprosessien sertifioinnin tarpeellisuudesta yrityksille. Kappaleessa 3 käydään läpi tietoturvan ja tietoturvan hallinnan merkitystä yrityksille. Tietoturvalle asetetaan usein tavoitteita, jotka tulee saavuttaa ja tietoturvanhallinta kuvataan jatkuvaksi palveluntoimitusprosessiksi. Kappaleessa 4 käydään läpi, miten tietojärjestelmiin liittyviä identiteettejä hallinnoidaan ja miten eri hallintamenetelmät eroavat toisistaan. Kappaleessa 5 käydään läpi, mitä tarkoitetaan pääsynhallinnalla. Pääsynhallintamenetelmän valintaan vaikuttaa oleellisesti se, mitä sillä halutaan saavuttaa.

Kappaleessa 6 käydään tapaustutkimuksena läpi, miten pääsynhallintamenetelmät on toteutettu IT-ulkoistuspalveluita tarjoavassa yrityksessä. Kappaleessa käydään läpi yrityksen pääsynhallinnassa käytetyt menetelmät ja työkalut sekä pyritään osoittamaan havaitut ongelmakohdat.

Kappale 7 esittelee toteutusehdotuksen siitä, miten pääsynhallinta voitaisiin toteuttaa IT-ulkoistuspalveluita tarjoavassa yrityksessä. Pääsynhallinta pyritään kuvaamaan siten, että se voitaisiin määrittää yhdeksi palvelutoiminnoista. Toteutusehdotuksen tavoitteena on tarjota tehokas tapa hallinnoida ja toteuttaa käyttöoikeus-

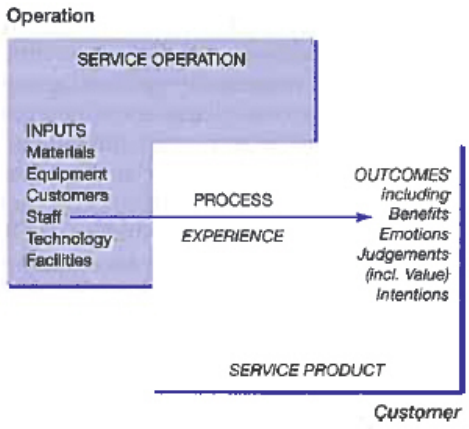
pyyntöjä ja osaltaan lisätä yrityksen tietoturvaa.

Kappale 8 sisältää toteutusehdotuksen arviointiosuuden ja yhteenvedon tutkimuksesta. Tuloksia vertaillaan asetettuihin arviointikriteereihin ja tapaustutkimuksesta saatuihin tuloksiin. Lisäksi käydään läpi kehitysehdotukset ja jatkotutkimus.

2 Palvelunhallinta IT palveluorganisaatiossa

Palvelulla voidaan tarkoittaa monia eri asioita, ja sen tarkoitus riippuu vahvasti asiayhteydestä. Joillekin palvelu tarkoittaa asiakaspalvelua ja joillekin logistista tai taloudellista toimintaa. Tässä diplomityössä palvelulla tarkoitetaan yhtä tai useampaa vuorovaikutusaktiviteettia asiakkaiden ja palveluresurssien välillä. Palveluaktiviteeteilla pyritään vastaamaan asiakkaan pyyntöihin ja tarjoamaan niitä tuloksia, joita asiakas haluaa saavuttaa. Lisäarvoa pyritään tuottamaan vapauttamalla asiakas riskeistä ja kustannuksista, joita tulosten tuottaminen edellyttää, laskuttamalla asiakasta vain palvelun käytöstä. Palvelun tarjoamisen yhteydessä asiakkaalla tarkoitetaan osapuolta, joka pyytää palvelua, ottamatta kantaa onko hän organisaation sisäinen henkilö, partneri tai ulkoinen asiakas. [7, s. 9]

Palvelun tuottamiseen on usein määritelty prosessi, jonka mukaan palvelua tuotetaan. Palvelun tuottaminen lähtee liikkeelle syötteestä (engl. input) ja päättyy tulokseen (output). Asiakas ei välttämättä näe tai koe koko palvelun tuottamiseen vaadittua työmäärää ja prosessia vaan ainoastaan toiminnot ja palautteet, joihin hän on osallisena sekä suorittamiseen kuluneen ajan ja saadut tulokset. Kuvassa 1 on kuvattu etualalle asiakkaan näkemä ja kokema osa palvelusta ja taka-ala pitää sisällään palvelun tuottamiseen liittyviä työtehtäviä ja prosesseja, joita asiakas ei tavallisesti näe ja koe. Palvelun prosessin ja asiakkaan kokemuksen päällekkäisyys yhdistettynä IT-palveluiden abstraktiin luonteeseen tekevät palveluiden hallinnasta erityisen haasteellista, jännittävää ja ajoittain jopa turhauttavaa. Palveluiden suunnittelussa ja kehityksessä tulee kiinnittää huomiota prosessin tehokkuuden lisäksi myös asiakkaan saamaan kokemukseen, koska sillä on suuri vaikutus asiakkaan saamaan laatuvaikutelmaan koko organisaatiosta. Palvelun kannalta asiakkaaksi luetaan osapuoli, joka joko käyttää palvelua tai vastaanottaa sen lopputuleman. Osapuoli voi olla organisaation sisäinen tai ulkoinen. Tässä diplomityössä asiakkaalla tarkoitetaan ensisijaisesti osapuolta, joka ostaa palvelua palveluntarjoajayritykseltä. [7, s. 10]



Kuva 1: Palvelutoiminta. [7, s. 11]

Palvelunhallinta (engl. Service Management) on kokonaisuus organisatorisia erikoiskykyjä tarjota asiakkaalle arvoa palveluiden muodossa. Kyvyt ovat toimintoja ja prosesseja, joilla hallitaan palveluita niiden elinkaaren ajan keskittyen erityisesti palveluiden strategiaan, suunnitteluun, siirtymävaiheeseen, käyttöön ja jatkuvaan parantamiseen. Kyvykkyydet myös ilmaisevat palveluorganisaation kapasiteettia, pätevyyttä ja luottamuksellisuutta. Ilman näitä kyvykkyyksiä ja taitoa muuttaa organisaation resursseja arvoa tuottaviksi palveluiksi, palveluorganisaatio on ainoastaan joukko resursseja, joilla itsellään on suhteellisen alhainen todellinen arvo asiakkaalle. [2, s. 11]

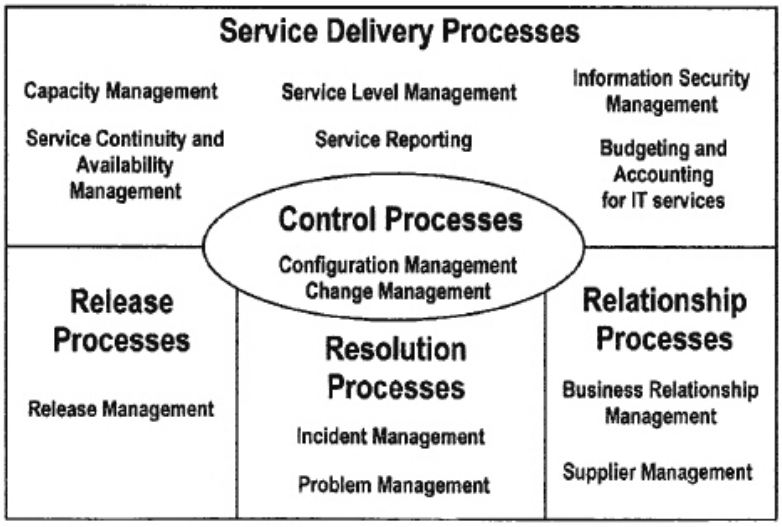
Palvelunhallinnan tärkeys korostuu IT-palveluita tarjoavassa organisaatiossa, sillä tarjottujen palveluiden määrän ollessa suuri toimintojen toistettavuus, tehokkuus, standardien noudattaminen ja skaalautuvuus vaikuttavat oleellisesti palveluiden kustannusten ja laadun hallintaan [17]. IT-palveluntarjoajan liiketoiminnan vaatimukset usein edellyttävät palvelujen toimittamisen olevan kustannustehokasta, ja liiketoiminnan jatkuvuuden kannalta palveluiden laadun tulee täyttää asiakkaiden asettamat kriteerit [9, s. 1].

Palvelunhallinnan päätavoitteita ovat [8, s. 4]:

- Sovittaa IT-palvelut yrityksen oman liiketoiminnan sekä asiakkaiden nykyisiin ja tuleviin tarpeisiin
- Parantaa tuotettujen IT-palveluiden laatua ja asiakkaan saamaa kokemusta palvelusta
- Vähentää palvelun ylläpitämiseen vaadittavia kustannuksia

ISO/IEC 20000-1:2005 määrittelee kuvan 2 mukaisesti palvelunhallintaprosessit viiteen kategoriaan [9, s. 1]:

1. Palveluntoimitusprosessit (engl. Service Delivery Processes)
2. Yhteysprosessit (engl. Relationship Processes)
3. Ratkaisuprosessit (engl. Resolution Processes)
4. Julkaisuprosessit (engl. Release Processes)
5. Kontrolliprosessit (engl. Control Processes)



Kuva 2: Palvelunhallintaprosessit. [9, s. 1]

Tässä diplomityössä tarkasteltu pääsynhallinta on vahvasti yhteydessä tietoturvanhallintaprosessiin. Tietoturvan hallintaprosessi on ISO/IEC 20000-1:2005:n mukaan yksi palveluntoimitusprosesseista. Pääsynhallintaprosessilla on tarkoitus luoda lisäarvoa yritykselle tarjoamalla keskitetysti hallittuja ja kustannustehokkaita pääsyn anomis- ja toimitusaktiviteetteja [1, s. 68].

2.1 Sertifioinnin tarpeellisuus

Organisaation rakennettua toimintaprosessinsa ja -politiikkansa perustuen yleisesti hyväksyttyihin alan parhaisiin käytäntöihin (ITIL v3, COBIT Guidance to Achieve Control Objectives for Successful IT Governance), organisaatio voi hakea muun muassa ISO 9001 laadunhallinnan-, ISO/IEC 20000 palveluidenhallinnan- ja ISO/IEC 27001 tietoturvahallinnan standardien mukaisia sertifiointeja koko toiminnalleen tai jollekin toiminnan osa-alueelle. [14]

Standardien tarkoitus on mahdollistaa systemaattinen tapa ohjata ja hallita organisaation toimintoja ja prosesseja. Standardien noudattaminen auttaa organisaatiota paremmin ymmärtämään ja täyttämään asiakkaiden ja muiden sidosryhmien tarpeet ja odotukset sekä valvomaan ja kehittämään toimintansa laadun- ja tietoturvanhallintajärjestelmiä. [18]

Toiminnan sertifiointi on kolmannen osapuolen antama pätevä todiste, joka osoittaa yrityksen sitoutumisen toimimaan vaatimusten mukaisesti [19]. Se lisää asiakkaiden ja yhteistyökumppaneiden luottamusta organisaatioon ja voi vaikuttaa positiivisesti organisaation liiketoiminnan jatkuvuuteen [3, s. 11-12].

3 Tietoturva

Organisaatioiden tärkeimpiä pääomia ovat tieto ja tietojärjestelmät [4, viii]. Tieto ja tiedon hallinta vaikuttavat oleellisesti liiketoiminnan jatkuvuuteen ja kasvuun, sillä tietoon kohdistuvalla rikoksella tai vahingolla voi olla organisaation tulevaisuuden kannalta suuremmat vaikutukset kuin etukäteen tulee ymmärtäneeksi [3, s. 1]. Tietoturvan vaarantuessa vaikutukset ulottuvat liiketoiminnan kilpailukykyyn, taloudelliseen kannattavuuteen ja organisaation maineeseen [3, s. 1].

Tieto voi esiintyä monessa muodossa. Se voi olla esimerkiksi paperille tulostettua, keskustelussa puhuttua, videolla näytettyä, postissa lähetettyä tai sähköiseen järjestelmään kuten tietokantaan tallennettua. Riippumatta tiedon esitys- ja tallennusmuodosta, tiedon tulee olla aina asianmukaisesti suojattu. [4, viii]

Tietoturvan tärkeys on korostunut erityisesti liiketoimintaympäristöjen liitäntöjen ja tietoturvauhkien määrän kasvaessa tietoyhteiskunnassa [4, viii]. Organisaatioiden valveutuneisuus tietoturvauhkia kohtaan on lisääntynyt ja tietoturva on otettu huomioon myös monissa standardointielimissä [3, s. 1]. Noudattamalla tietoturvastandardeja organisaatiot pyrkivät luomaan itselleen tietoturvan hallintajärjestelmän. Tietoturvan hallinnan tavoitteena on auttaa organisaatiota suojaamaan sen liiketoiminnan kannalta tärkeät tietopääomat ja järjestelmät [3, s. 1] [4, viii]. Tietoturvassa on pohjimmiltaan kyse riskien hallinnasta ja niiden arvioinnista. Suojattavalle tiedolle on osattava määritellä arvo, valittava hyväksyttävä riskitaso ja verrattava arvoa ja riskitasoa tietoturvainvestointeihin [6, s. 8].

Yksi yleisesti käytössä olevista tietoturvastandardeista on ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management, joka on kehitetty vuonna 1995 julkaistusta BS7799 tietoturvastandardista [4, iii]. ISO/IEC 27002:2005 tietoturvastandardi tarjoaa yleisiä periaatteita ja toimintamalleja organisaation tietoturvan hallinnan aloittamiseen, toteuttamiseen, huoltamiseen ja parantamiseen [4, s. 1]. Standardi koostuu kokoelmasta hyväksi havaittuja toimintamalleja ja -tapoja ja se keskittyy yleiseen liiketoiminnan turvaamiseen tähtäävään tietoturvaan [4, s. 1].

3.1 Tietoturvan hallinta

Tietoturvan toteutuksen tulee aina perustua tietoturvapolitiikkaan, jonka laadinnassa tulisi käyttää riskianalyysin tuloksia [4, s. 7]. Tietoturvapolitiikan tarkoituksena on tarjota ohjausta ja tukea koko organisaatiolle sekä sen hallinnolle ja johdolle toimia liiketoiminnan vaatimusten ja asianmukaisten lakien ja määräysten mukaisesti [4, s. 7]. Organisaation johdon tulee asettaa selkeä poliittinen suunta, joka tukee liiketoiminnan tavoitteita ja joka osoittaa sitoutumista tietoturvan ja sen politiikan ylläpitämiseen koko organisaatiossa [4, s. 7]. Tietoturvapolitiikassa määritellään käytännön tietoturvan hallinnan vastuualueet sekä raportointitoimenpiteet, joita tulee

noudattaa havaittaessa mahdollisia tietoturvarikkomuksia [3, s. 4].

Tietoturvan hallinnan prosessin päämääränä on yhdenmukaistaa linja tietotekniikan tietoturvan ja yritystietoturvan välillä ja taata tietoturva, joka on tehokkaasti hallittavissa kaikissa palveluissa ja palvelunhallinta toiminnoissa. Tietoturvan hallinta toimii osana organisaation hallintoa, jonka tarkoituksena on tarjota strategisia neuvoja tietoturvatoiminnoille ja varmistaa toimintojen tavoitteiden saavuttaminen. Tietoturvan hallinta pyrkii takaamaan, että tietoturvariskit tunnistetaan ja niihin reagoidaan asianmukaisesti ja yrityksen tietoresursseja käytetään vastuullisesti. [2, s. 141]

Tietoturvan hallinta on saavutettavissa ottamalla käyttöön asianmukaiset toimintatavat sisältäen politiikan, prosessit, käytännöt, organisaatiorakenteet ja ohjelmistoja laitteistotoiminnot [2] [4]. Tietoturvan hallinnan aloittamisen tueksi ja ohjeistukseksi on määritelty erinäisiä standardeja, viitekehyksiä ja parhaita käytäntöjä sisältäviä julkaisuja. Tällaisia standardeja ja julkaisua ovat muun muassa:

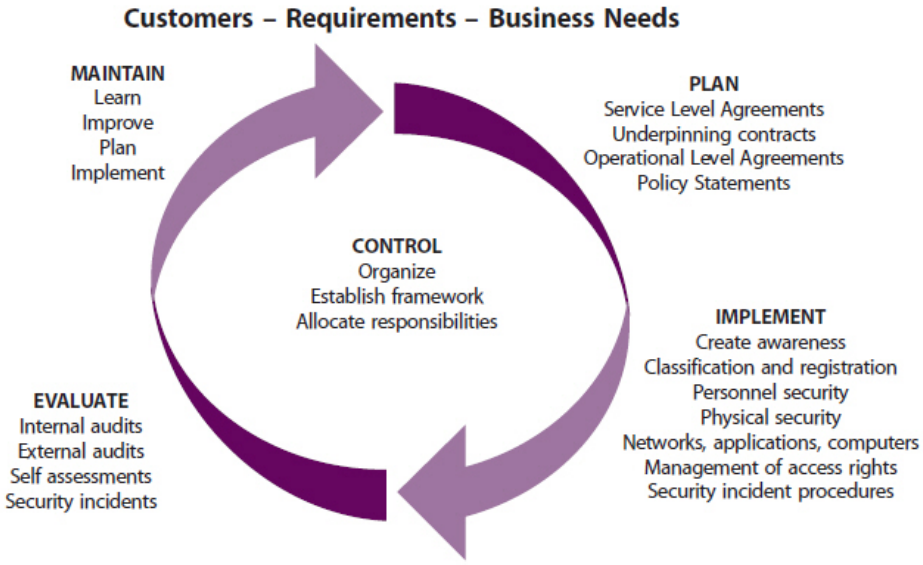
- Standardi ISO 27002:2005, joka tarjoaa yleisiä periaatteita, toimintamalleja ja käytäntöjä tietoturvan hallinnan käyttöönottoon. [4, s. 1]
- Standardi ISO 27001:2005, joka määrittelee vaatimuksia dokumentoidun tietoturvan hallinnan perustamiseen, toteuttamiseen, käyttämiseen, valvomiseen, arvioimiseen ja parantamiseen. [5, s. 1]
- ITIL v3 Service Design, maailmanlaajuisesti tunnettu prosessikehys, joka tarjoaa laajan kokoelman käytäntöjä IT-palveluiden kehitykseen, hallintaan ja johtamiseen. [2]

Organisaation valveutuneisuus olemassa olevista tietoturvista on yksi tärkeimmistä tietoturvallisuuden lisäämisen ajajista ja tietoturvan hallinnon käyttöönottamisen syistä [3, s. 1]. Useimmille organisaatioille tietoturvatavoitteiden saavuttaminen edellyttää tiettyjen ehtojen täyttymistä [2, s. 141]:

- Saatavuus: Tieto on saatavilla ja käytettävissä aina tarvittaessa, ja järjestelmä kykenee asianmukaisesti torjumaan ja toipumaan hyökkäyksistä ongelmatilanteiden ehkäisemiseksi.
- Luottamuksellisuus: Tieto on noudettavissa ja luovutetaan vain heille, joilla on oikeus tietoon.
- Eheys: Tieto on yhtenäistä ja täsmällistä, sekä suojattu epätoivotulta muokkaukselta.
- Aitous ja kiistämättömyys: Yrityksen liiketoimintatapahtumat ja tiedon vaihtaminen erilaisten osapuolten välillä ovat luotettavia ja voidaan todentaa jälkikäteen.

Tietoturvan hallintaprosessin voidaan kuvata koostuvan kuvan 3 mukaisesti viidestä osasta [2, s. 144]:

1. Kontrolli: määrittelee vastuualueet, luo ja hallinnoi dokumentaatioita, perustaa hallinnollisen viitekehyksen organisaation tietoturvan hallinnalle.
2. Suunnittelu: suunnittelee ja suosittelee asianmukaisia turvatoimia, jotka perustuvat organisaation asettamiin vaatimuksiin.
3. Käyttöönotto: varmistaa, että asianmukaiset menettelyt, työkalut ja kontrollit ovat otettu käyttöön tukemaan tietoturvapolitiikkaa.
4. Arviointi: valvoo ja tarkistaa tietoturvapolitiikan ja -vaatimusten noudattamisen palvelutason (SLA) ja operatiivisen tason (OLA) sopimuksissa, suorittaa säännöllisiä tietoturvatarkastuksia tietojärjestelmiin ja tarjoaa tarvittaessa tietoa ulkoisille tarkastajille ja valvojille.
5. Ylläpito: parantaa SLA ja OLA sopimuksissa olevia turvallisuuden kannalta tärkeitä asioita sekä tehostaa turvatoimenpiteiden ja kontrollien käyttöönottoa.



Kuva 3: Tietoturvan hallinnan viitekehys. [2, s. 144]

3.1.1 Tehtävien eriyttäminen (SoD)

Tehtävien eriyttäminen (engl. separation of duties, SoD) on tietoturvaperiaate, jolla pyritään estämään mahdollinen haitallinen toiminta kohdejärjestelmiin. SoD periaate on, ettei yhdelläkään yksittäisellä käyttäjällä olisi mahdollisuutta suorittaa kaikkia toimenpiteitä itse tietyn kokonaisuuden sisällä. Esimerkiksi kaupankäyntiin tai

hankintaan liittyvissä ostoehdotuksissa käyttäjän ei tule pystyä itse hyväksymään tekemiään ostoehdotuksia. [22]

SoD voi olla joko staattinen tai dynaaminen [22]. Staattisessa tehtävien eriyttämisessä (SSD) roolijäsenyydet määritellään toisensa poissulkevina [23]. Dynaaminen tehtävien eriyttäminen (DSD) mahdollistaa päällekkäisyydet rooleissa, mutta rajoittaa roolien toimintoja saman tapahtuman sisällä [23]. Esimerkiksi käyttäjä voi olla sekä ostoehdotuksen tekijän että hyväksyjän roolissa, mutta käyttäjää estetään hyväksymästä hänen omia pyyntöjään [23].

3.1.2 Pienimmän oikeuden periaate

Pienimmän oikeuden periaate (engl. principle of least privilege) pyrkii estämään tahallisen ja tahattoman haitallisen toiminnan sallimalla käyttäjälle vain ne oikeudet, joita hän oikeasti tarvitsee työnsä suorittamiseen [22]. Pienimmän oikeuden periaatetta on verrattu tietoturvan kannalta yhtä merkittäväksi kuin tiedon eheyttä [24]. Pienimmän oikeuden periaate edellyttää käyttäjän työnkuvan kartoittamisen ja työnsuorittamiseen tarvittavien oikeuksien vähimmäistasojen määrittämisen [22].

4 Identiteetinhallinta

Ihmisen työtehtävien automatisointi ja automatisoinnin kehitys tietojärjestelmissä on johtanut tarpeeseen kyetä esittämään identiteettejä, jotka käyttävät mallina oikean elämän kokonaisuuksia ja vuorovaikutuksia. Tietojärjestelmissä identiteetin käsitys ja käyttö kehittyi yksinkertaisesta tunnistemäärittееstä tunnisteeksi, joka voi osoittaa useaan tuntomerkkiin ja niihin liitettyihin oikeuksiin, yleisesti viitaten profiiliin. Identiteetillä tarkoitetaan niitä tietoja, jotka erottavat yksilön ja todentavat hänen asemansa organisaatiossa. Identiteetti on aina yksilöllinen. Profiililla tarkoitetaan identiteetin digitaalista esittämistä, viitaten usein vain tiettyyn käyttäjään, mutta se voi olla myös esitys tietyn tyyppisestä käyttäjämallista, jolloin profiili voidaan siirtää käyttäjältä toiselle. [10, s. 40]

Identiteetinhallinta pyrkii vastaamaan haasteisiin, jotka liittyvät identiteettien ja profiilien määrän nopeaan kasvuun yritysten erilaisissa käyttöympäristöissä [11, s. 3]. Tällaisia haasteita ovat muun muassa ristiviittaukset profiilien välillä, jotka edustavat samaa identiteettiä, sekä näiden profiilien ominaisuuksien välinen synkronointi [10, s. 40]. Lisäksi turvallisen tietoympäristön ylläpito ja käyttö perustuvat identiteettien tunnistamiseen ja jaettujen käyttöoikeuksien hallintaan [10, s. 40]. Identiteetinhallinnassa tulee myös ottaa huomioon käytettävyyden säilyttäminen niin loppukäyttäjän kuin ylläpidon osalta [11, s. 3].

Identiteetinhallintaan liittyviä malleja löytyy kirjallisuudesta useita [10] [11] [28] [29] [30]. Pääsääntöisesti tietojärjestelmissä identiteetinhallintamenetelmät voidaan jakaa identiteettien hallinnollisen ja toiminnallisen laajuuden mukaan [10, s. 51]. Messaoud Benantar jakaa identiteetinhallintamenetelmät neljään luokkaan [10, s. 51]:

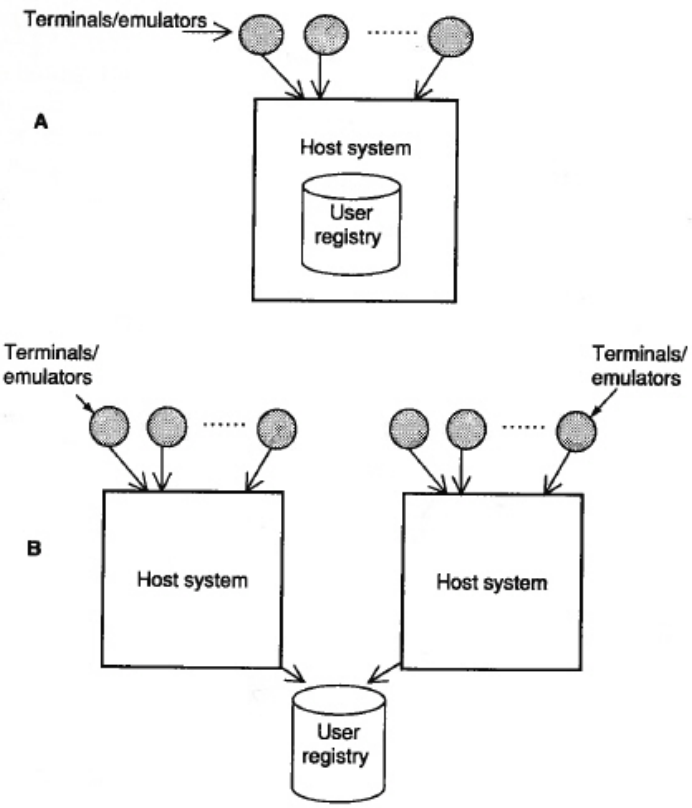
1. Paikallinen identiteetti (engl. Local identity)
2. Verkkoidentiteetti (engl. Network identity)
3. Yhdistetty identiteetti (engl. Federated identity)
4. Globaali Web identiteetti (engl. Global Web identity)

4.1 Paikallinen identiteetti

Käyttäjärekisterin ylläpitämistä ja hallinnoimista keskitetysti yhdessä järjestelmässä kutsutaan paikallisen identiteetin malliksi (engl. local identity) [10, s. 41]. Paikallisen identiteetin mallista käytetään myös nimeä eriytetyn identiteetin malli (engl. isolated identity) [28, s. 3]. Jokaiselle käyttäjälle, joka haluaa käyttää järjestelmää, tulee luoda yksilöllinen identiteetti käyttäjärekisteriin [10, s. 41] [28, s. 3]. Käyttäjärekisterissä käytettyjen identiteettien nimiavaruus on litteä, mistä johtuen kahta samannimistä identiteettiä ei voi olla järjestelmässä, vaan jokaisen identiteettinimen

tulee olla uniikki [10, s. 41]. Identiteettien lisäykset ja poistot ovat erillisiä tapahtumia, joilla ei ole vaikutusta muihin identiteetteihin [10, s. 41]. Hallinnoitavat oikeudet ovat kytköksissä oikeuksiin, joita käyttäjällä voi olla järjestelmän resursseihin [10, s. 41].

Keskitettyä käyttäjärekisteriä voi käyttää joko yksi (Kuva 4, kohta A) tai useampi kohdejärjestelmä (Kuva 4, kohta B). Jakamalla käyttäjärekisteri usean kohdejärjestelmän käytettäväksi pyritään lievittämään ylimääräistä järjestelmäkohtaista käyttäjärekisterin hallintaa. [10, s. 42]



Kuva 4: Paikallinen identiteetti [10, s. 40]

Paikallisen identiteetin hyöty on sen yksinkertaisuus. Identiteetin luominen käyttäjärekisteriin ja sen tunnistaminen ovat yksinkertaisia paikallisia prosesseja. Litteän nimiavaruuden rakenne on samanlainen kuin datarakenteen, jossa tietueet ovat taulukossa. Yksinkertaisen rakenteen vuoksi tietueita voidaan helposti hallita yksittäisinä kokonaisuuksina. [10, s. 42]

Paikallisen identiteetin mallin ongelmat ovat sen rajoitettu skaalautuvuus [28, s. 4], litteän nimiavaruuden rajoitukset sekä usean käyttäjärekisteriä käyttävän järjestelmän hallinnolliset haasteet [10, s. 43]. Rajoitettu skaalautuvuus kapasiteetin osal-

ta tulee ilmeiseksi käyttäjien ja järjestelmässä käytettävien osajärjestelmien määrän kasvaessa [10, s. 43]. Järjestelmän tulee pystyä tallentamaan ja ylläpitämään jokaisen järjestelmän tietueen tiedot, jolloin tietueiden suuri määrä saattaa vaikuttaa koko järjestelmän suorituskykyyn [10, s. 43]. Käyttäjäryhmien käyttäminen ei ratkaise skaalautuvuuteen liittyviä ongelmia, sillä identiteetin määrittely tapahtuu kuitenkin erillään riippumatta ryhmäjäsenyydestä [10, s. 43].

Litteän nimiavaruuden rakenne rajoittaa identiteettien nimeämisiä siten, että jokaisen identiteettinimen tulee olla uniikki, mikä johtaa usein siihen, että identiteettien nimet generoidaan järjestelmässä. Lisäksi paikallisen identiteetin mallissa identiteetin käytön laajuus rajoittuu niihin kohdejärjestelmiin, joihin se on määritelty. Kohdejärjestelmien, jotka käyttävät omaa käyttäjärekisteriä (Kuva 4, kohta A), määrän kasvaessa, myös identiteetteihin liitettyjen järjestelmäkohtaiset salasanojen määrä kasvaa. Tämä lisää käyttäjien muistikuormaa ja samalla heikentää palveluiden tehokasta käyttämistä. [10, s. 43]

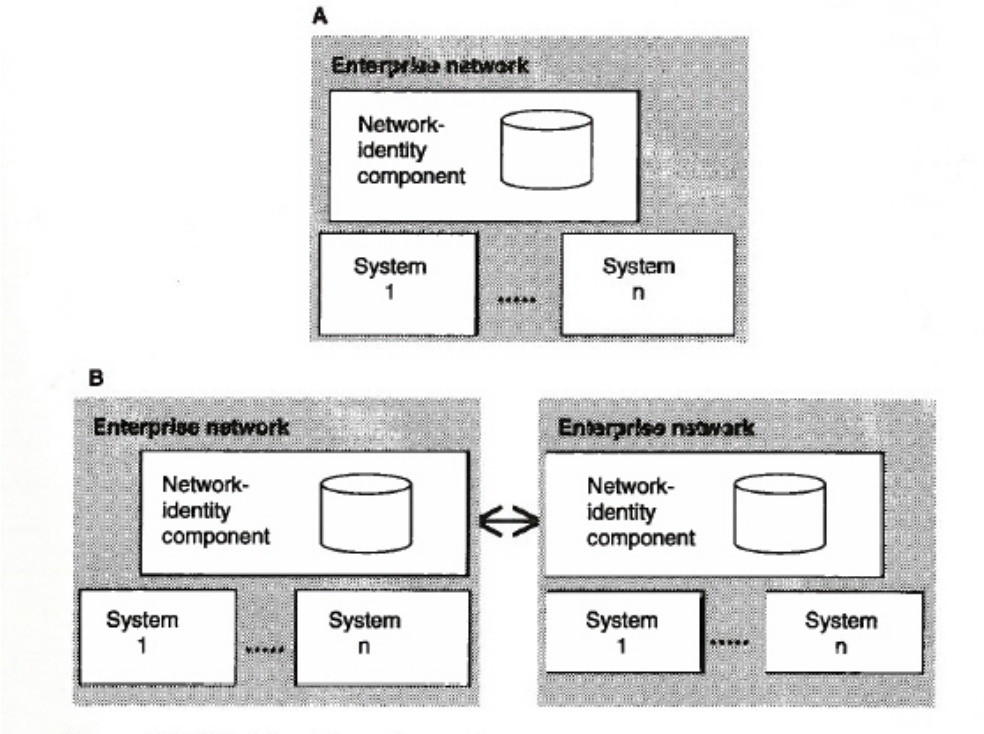
Salasanasynkronisointi on yksi vaihtoehto korvaamaan järjestelmäkohtaisia salasanoja [10, s. 43]. Salasanasynkronoinnin idea on, että käyttäjällä on vain yksi salasana ja se synkronisoidaan käyttäjärekisterien välillä. Toisin kuin kertakirjautumismenetelmässä (SSO), salasanasynkronisointia käytettäessä käyttäjän tarvitsee jokaiseen palveluun kirjautuessa syöttää aina salasana [10, s. 43]. Salasanasynkronisoinnin käyttöönotto on usein kuitenkin helpompaa kuin SSO:n, sillä se ei vaadi suuria muutoksia yrityksen olemassa oleviin tietoverkkorakenteisiin [10, s. 43]. Salasanasynkronoinnin haittana on käyttäjärekisterissä olevien muiden käyttäjätietojen yhteneväisyyden ylläpitäminen [10, s. 43]. Salasanasynkronointia vastaava toimintatapa on metaidentiteetti, jossa tietyt identiteettiin liitetyt jaetaan järjestelmien ja käyttäjärekisterien kesken [28, s. 6].

Toinen vaihtoehto on käyttää jaettua käyttäjärekisteriä usean kohdejärjestelmän kesken (Kuva 4, kohta B) [10, s. 44]. Kirjallisuudessa jaetun käyttäjärekisterin toimintatavasta käytetään myös nimeä yhteinen identiteetti (engl. common user identity model) [28, s. 5]. Jaetun käyttäjärekisterin käyttämisen etuna salasanasynkronointiin verrattaessa on käyttäjätietojen eheys ja helppo ylläpidettävyys, mutta käyttäjämäärän ja rekisteriä käyttävien järjestelmien määrän kasvaessa suorituskyky voi osoittautua pullonkaulaksi [10, s. 44].

4.2 Verkkoidentiteetti

Tietoverkkojen ja hajautettujen tietojärjestelmien yleistyminen on johtanut verkkoidentiteetin mallin (engl. network identity) syntymiseen. Verkkoidentiteetin mallissa identiteettiä ei autentikoida yksittäistä kohdejärjestelmää kohden, vaan autentikointi tapahtuu tietoverkkoa kohden. Kun identiteetti on vahvistettu tietoverkkoa kohden, verkkoon liitetyt resurssit ja palvelut ovat käytettävissä ilman, että identiteettiä tarvitsee erikseen vahvistaa. Verkkoidentiteetin laajuus on perinteisesti rajoitet-

tu yrityksen omaan verkkoon (Kuva 5, kohta A), mutta se on mahdollista laajentaa myös usean erillisen verkon tai yrityksen käyttöön (Kuva 5, kohta B). [10, s. 46]



Kuva 5: Verkkoidentiteetin malli [10, s. 46]

Tyypillinen esimerkki verkkoidentiteetistä on tietokoneen käyttöjärjestelmätunnuksien käyttäminen verkkotunnuksina ja niiden hallinnointi esimerkiksi *Microsoft Active Directoryn* avulla [31]. *Active Directory* toimii verkon identiteettikomponenttina, sisältäen käyttäjätietokannan ja hakemistopalvelut sekä tiedot verkon resursseista [32]. Se mahdollistaa keskitetyn resurssien jakamisen käyttäjille ja sovelluksille [32].

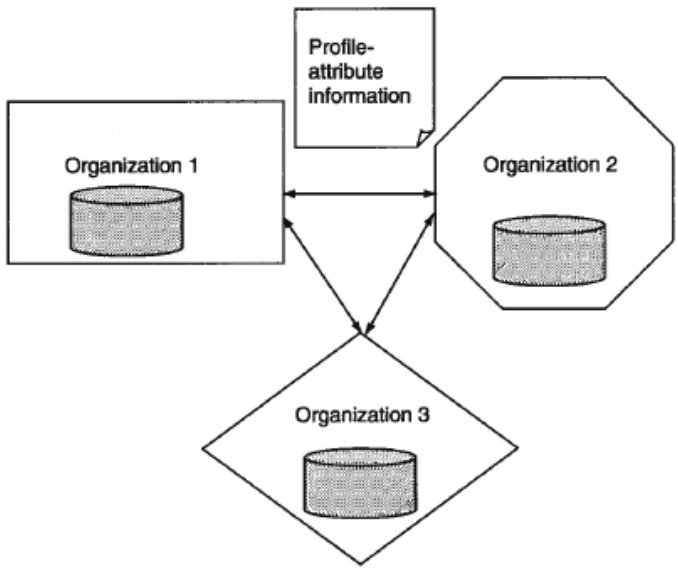
Verkkoidentiteetti on tehokas tapa tarjota suuri määrä palveluita suurelle määrälle käyttäjiä. Verkkoidentiteetin ongelma on, että identiteettikohtaiset resurssienkäyttömahdollisuudet ovat usein todella suuret, jolloin myös tietoturvaan kohdistuvien uhkien määrä kasvaa. Lisäksi jos identiteetin vahvistaminen onnistutaan kokonaan kiertämään, saa pahantahtoinen käyttäjä mahdollisesti rajattoman pääsyn koko verkon resursseihin. [11]

4.3 Yhdistetty identiteetti

Yhdistetty identiteetti (engl. federated identity) perustuu identiteettien yhdistämiseen sovitun liittouman kesken, kuten kahden tai useamman yrityksen tai palveluntarjoajan välillä [28, s. 4]. Yhdistetystä identiteetistä käytetään kirjallisuudessa myös nimeä yhteinen käyttäjäntunnistus [33]. Vaikka identiteettirekisterien tiedot voidaan säilyttää uniikkeina omissa ympäristöissä, voidaan liittouman kaikkien osapuolten identiteettejä käyttää tunnistautumiseen [28, s. 4] [29]. Yhdistetty identiteetti mahdollistaa liittouman osapuolten tarjota pääsyä suurelle määrälle käyttäjiä ilman, että heidän tarvitsee yksin hallita ja ylläpitää koko identiteettiavaruutta ja niiden ominaisuuksia [28, s. 4]. Ehtona yhdistetyn identiteetin käyttämiselle on yritysten välinen luottamus [10, s. 47] [29].

Yhdistetty identiteetti mahdollistaa myös kertakirjautumismenetelmän käytön (SSO) kaikkien osapuolten palveluiden välillä [10, s. 47]. SSO menetelmässä käyttäjä kirjautuu vain yhteen palveluun, jonka jälkeen erillistä kirjautumista ei enää tarvita muiden osapuolten palveluiden käyttöön [28, s. 4] [11, s. 2]. Autentikointitieto välitetään muille osapuolille identiteetin kotirekisteristä osapuolten hyväksymää turvallista ja luottamuksellista kanavaa pitkin [10, s. 47]. Toimintatapa mahdollistaa läpinäkyvyyden osapuolten palveluiden ja käyttäjien välillä [10, s. 47]. Loppukäyttäjän ei tarvitse olla tietoinen taustalla olevista prosesseista eikä hänen tarvitse rekisteröityä jokaisen osapuolen kanssa [10, s. 47].

Kuvassa 6 on ylätason malli yhdistetystä identiteetistä. Erimuotoiset kehykset yritysten ympärillä kuvaavat yritysten ylläpitämiä omia identiteetinhallintamalleja, jotka voivat olla riippumia muiden ylläpitämistä hallintamalleista.



Kuva 6: Yhdistetty identiteetti [10, s. 50]

Ero yhdistetyn identiteetin ja jaetun paikallisen identiteetin välillä on, että yhdistetyssä identiteetissä osapuolet ylläpitävät omia käyttäjärekistereitä ja tunnistautumistapoja, kun taas jaetussa paikallisessa identiteetissä on yksi käyttäjärekisteri ja tunnistautumistapa, jota osapuolet käyttävät. Ongelmana yhdistetyn identiteetin mallissa on yhteisten käytäntöjen ja tietoturvapolitiikan hyväksyminen ja luottamussuhteiden rakentaminen. Esimerkiksi autentikointitietojen valvominen ja kontrollointi suuressa liittoumassa voi osoittautua haasteelliseksi, koska osapuolten tietoturvavaatimukset saattavat erota toisistaan. [11, s. 2]

4.4 Globaali verkkoidentiteetti

Globaali verkkoidentiteetti (engl. global web identity) kuvaa identiteettiä, joka on olemassa ja tunnistettavissa koko verkossa, esimerkiksi Internetissä, ja joka edustaa tiettyä kokonaisuutta samaan tapaan, kuin *Uniform Resource Identifier* (URI) edustaa ja on tunniste tietylle internet-resurssille [12]. Globaalin verkkoidentiteetin idea on, että identiteetti voidaan yksikäsitteisesti tunnistaa ja ottaa käyttöön niin paikallisesti kuin verkon muissa solmuissa [10, s. 51].

Muun muassa riittävän tieturvan ylläpitämisen, tarvittavien luottamussuhteiden rakentamisen ja puuttuvien standardien vuoksi ei globaalia verkkoidentiteettiä ole laajasti otettu käyttöön [11] [10]. Lupaavin globaalin verkkoidentiteetin toteutustapa perustuu XDI.ORG organisaation kehittämiin avoimiin standardeihin XRI (*Extensible Resource Identifier*) ja XDI (*XRI Data Iterchange*), jotka perustuvat XML:iin (*Extensible Markup Language*) [13]. Näillä on tarkoitus mahdollistaa organisaatioille

digitaalisen Internet identiteetin luominen [10, s. 54].

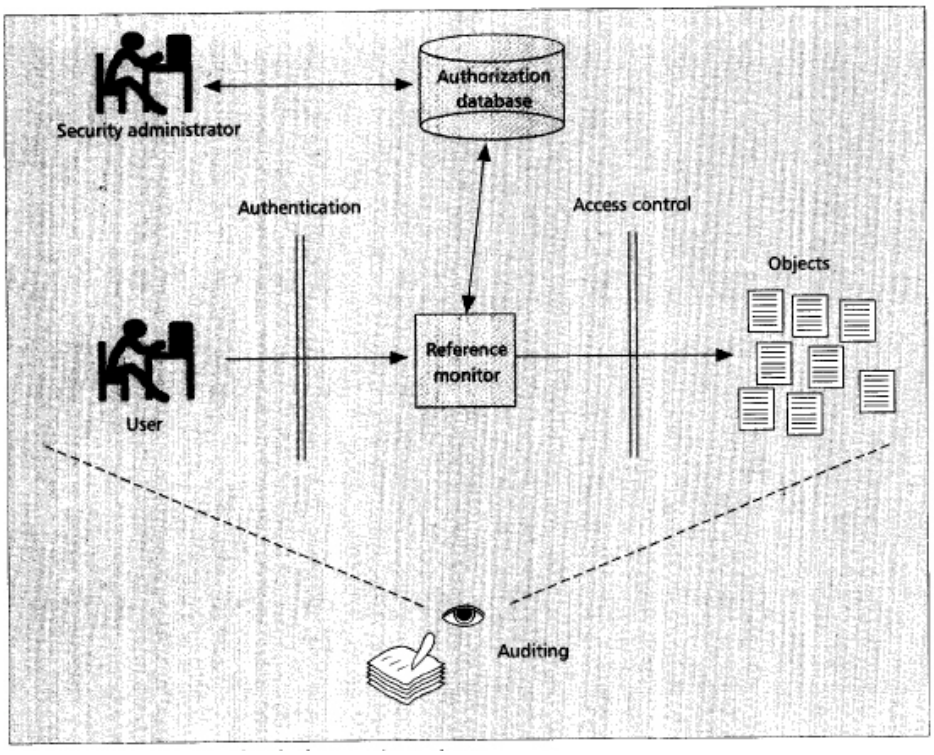
5 Pääsynhallinta

Pääsynhallinnan tarkoituksena on tarjota käyttäjille oikeus päästä ja käyttää tietoa ja IT-palveluita, joihin heillä on vahvistettu valtuus, kuitenkin eväten vahvistamattomien ja luvattomien käyttäjien pääsy palveluihin ja niiden käyttö [1, s. 68]. Pääsynhallinta auttaa suojaamaan tiedon luottamuksellisuuden, eheyden ja saatavuuden [1, s. 68] sekä pyrkii osaltaan estämään haitallisen toiminnan, joka voisi johtaa yrityksen tietoturvan vaarantumiseen [16, s. 40]. Tässä diplomityössä pääsynhallinnalla tarkoitetaan käyttäjien pääsy- ja käyttöoikeuksien hallintaa tietojärjestelmiin ja -ympäristöihin.

Tietoturvan- ja identiteetinhallinta ovat keskeisessä asemassa toimivan pääsynhallinnan toteuttamisen kannalta sillä pääsynhallintamenetelmät luottavat olemassa oleviin tietoturva- ja identiteetinhallintamenetelmiin ja pyrkivät toteuttamaan sovittua tietoturvapolitiikkaa [16, s. 40] [10, s. 20]. Lisäksi tietoturva- ja identiteetinhallinta osaltaan auttavat määrittelemään, onko tunnistetulla käyttäjällä oikeutta käyttää kohderesurssia. Resurssi voi olla mikä tahansa kohde, palvelu, tietojärjestelmä, palvelin tai tiedosto [10, s. 20]. Tässä diplomityössä käytetään termiä kohdejärjestelmä, sillä se kuvaa parhaiten kaikkia tietojärjestelmien sisältämiä kohteita.

5.1 Reference monitor -malli

Nykyiset pääsynhallintamenetelmät perustuvat Butler Lampsonin 1970-luvulla esittelemään *reference monitor* malliin [20]. *Reference monitor* on osa luotettua tietojenkäsittelypohjaa (TCB), ja se välittää pääsyn kohdejärjestelmiin sovitun turvapolitiikan mukaisesti [10, s. 21]. Politiikka voi olla toteutettu tulkitsemalla kohdejärjestelmä- ja käyttäjärekistereitä sääntöjen ja tuntomerkkien perusteella [10, s. 21]. Politiikkaa ylläpidetään valtuutustietokannassa (*authorization database*), josta *reference monitor* tiedustelee, onko yritetty pääsyoperaatio sallittu [16, s. 40]. Pääsyoperaatioihin voi olla liitettynä myös valvonta, joka pitää kirjaa olennaisista toiminnoista [16, s. 40]. Pääsynhallintaan liittyvät päätoiminnot on kuvattu kuvaan 7. Toimintojen eriytys todellisessa toteutuksessa ei ole aina selkeä, mutta niiden eriyttäminen edes loogisella tasolla auttaa hahmottamaan kokonaiskuvaa ja parantaa niiden hallittavuutta [16, s. 40].



Kuva 7: Yhdistetty identiteetti [16, s. 41]

Autentikoinnin ja pääsyn kontrolloinnin toiminnallisuuden eron ymmärtäminen on tärkeää vastuualueiden rajaamiseksi. Käyttäjän identiteetin tunnistaminen ja varmistaminen kuuluu autentikointipalveluiden vastuulle, ja ne ovat osa identiteetinhallintaa. Pääsyn kontrollointi olettaa, että käyttäjä on luotettavasti tunnistettu autentikointipalveluissa ja kyseessä oleva pääsyoikeus vahvistettu reference monitorin toimesta. Nämä toiminnot pelkästään eivät ole kattava ratkaisu järjestelmien turvaamiseen. Tietoturvanhallinta usein vaatii, että pääsynhallintaan on liitettynä myös valvonta tai kirjanpito, jonka avulla voidaan analysoida jälkikäteen järjestelmiin kohdistuvia pääsypyyntöjä ja aktiviteetteja. [16, s. 40]

Sopivan pääsynhallintamenetelmän valinta voi olla hankalaa ja yleisesti ei ole olemassa menetelmää, joka olisi parempi kuin muut; on olemassa menetelmiä, jotka tarjoavat korkeamman tietosuojatason kuin toiset. Toisaalta, kaikkia järjestelmiä eivät koske samat tietoturva- ja käytettävyysvaatimukset, jolloin tiukka pääsynhallintamenetelmä kriittiseen järjestelmään ei välttämättä sovellu ympäristöön, jossa vaaditaan joustavuutta ja käytettävyyttä. [16, s. 41]

5.2 Harkinnanvarainen pääsynhallinta (DAC)

Harkinnanvaraisessa pääsynhallinnassa (engl. discretionary access control, DAC) pääsy kohdejärjestelmään toteutetaan perustuen käyttäjän identiteettiin ja siihen

liitettyihin valtuuksiin tai sääntöihin, jotka määrittelevät yksittäisen käyttäjän tai käyttäjäryhmän oikeudet kohdejärjestelmään [16, s. 44]. DAC mallissa jokaiselle kohdejärjestelmälle on määritelty yksi tai useampi omistaja, jotka voivat täysin oman harkintansa mukaan määritellä muiden käyttäjien pääsy- ja käyttöoikeuksia kohdejärjestelmään [10, s. 25]. Lisäksi jokaisella käyttäjällä on oikeus hyväksyä pääsy heidän hallinnoimiinsa sovelluksiin kohdejärjestelmän sisällä ilman omistajan valtuutusta [16, s. 44]. DAC:n politiikka esiintyy muodossa tai toisessa lähes kaikissa pääsynhallintamenetelmissä, sillä resurssi-omistajuus malli pääsynhallinnassa on hyvin yleinen ja vastaa todellista maailmaa [10, s. 25].

DAC -menetelmän hyötyjä ovat yksinkertaisuus, joustavuus ja käyttöönoton helppous. Haittapuolena DAC ei tarjoa mitään oikeaa varmuutta tiedon kulusta, vaan pääsy- ja käyttöoikeuksien leviäminen on teoriassa rajoittamatonta ja vaikeasti ennustettavaa [10, s. 25]. Lisäksi pääsyrajoitukset on kohtuullisen helppo kiertää, sillä käyttäjät voivat sallia muille käyttäjille harkintavaltansa alaisia oikeuksia muiden tästä tietämättä [16, s. 44].

Menetelmää sanotaan suljetuksi tai avoimeksi riippuen reference monitorin oletuspäätöksestä pääsylle. Suljetussa menetelmässä pääsy annetaan vain jos pääsylle löytyy positiivinen valtuutus kohdejärjestelmään. Avoimessa menetelmässä puolestaan pääsy annetaan aina, ellei erillistä negatiivista valtuutusta pääsylle löydy. Positiivisia ja negatiivisia valtuutuksia voidaan käyttää samanaikaisesti, jolloin on mahdollista määritellä tarkemmin valtuutetut ja luvattomat pääsyt, mutta niiden samanaikainen ylläpito voi muuttua monimutkaiseksi. [16, s. 44]

5.3 Pakollinen pääsynhallinta (MAC)

Pakollisessa pääsynhallinnassa (engl. mandatory access control, MAC) pääsy kohdejärjestelmiin perustuu kohdejärjestelmien ja käyttäjien luokittelemiseen tietoturvatasoihin. Kohteeseen liitetty tietoturvataso kuvastaa kohteen sisältämän tiedon arkaluonteisuutta ja riskiä, minkä tiedon luvaton paljastuminen voisi aiheuttaa. Käyttäjään liitetty tietoturvataso, toisin sanoen pääsyoikeus, kuvastaa puolestaan käyttäjän luotettavuutta. [16, s. 44]

MAC -menetelmä kehittyi sotilashierarkian pohjalta ja soveltuukin erityisesti sotilaallisiin ja siviilihallinnon tarpeisiin [10, s. 25]. MAC turvatasojen hierarkia voidaan kuvata koostuvan esimerkiksi neljästä tasosta: Top Secret (TS), Secret (S), Confidential (C) ja Unclassified (U) [16, s. 44].

Päinvastoin kuin DAC:ssa, MAC mallissa ei käytetä resurssi-omistajuus mallia, vaan oikeudet määritellään hallinnollisin menettelyin etukäteen ja ne säilyvät muuttumattomina sen jälkeen. Pääsy- ja käyttöoikeuksien leviäminen ei ole mahdollista käyttäjien tai järjestelmien toimesta, vaan luotettu taho hallinnoi oikeuksia. MAC mahdollistaa ennustettavan ja yksisuuntaisen tiedonkulun. [10, s. 25]

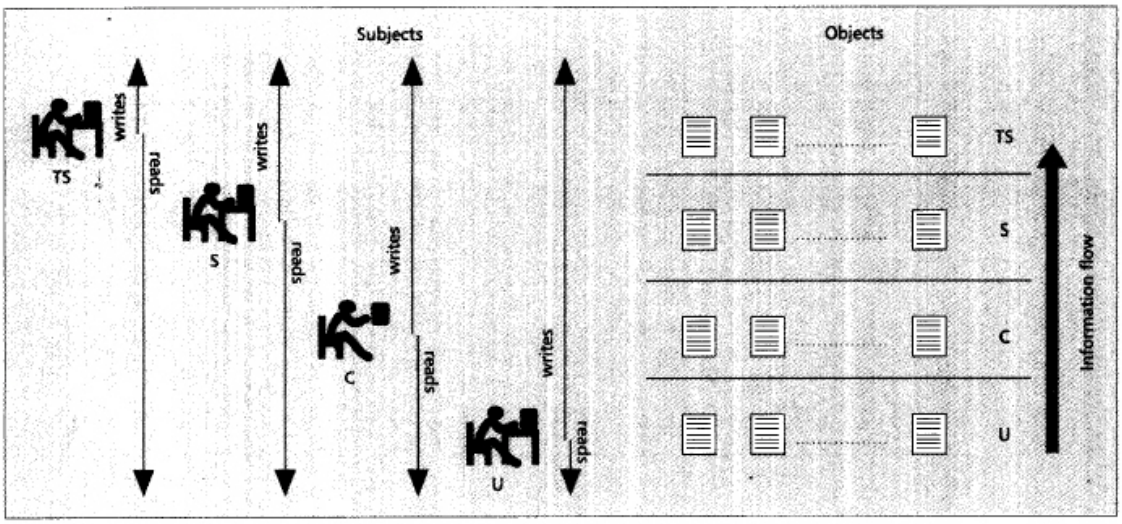
5.3.1 Bell-LaPadula -malli (BLP)

David Elliott Bell ja Leonard J. LaPadula kehittivät formaalin mallin kuvaamaan MAC menetelmän useita tietoturvatasoja [21]. Bell-LaPadula -malli (BLP) määrittelee kaksi tiedonkulkuun vaikuttavaa sääntöä [10, s. 137]:

1. *Simple security rule*, joka tunnetaan myös ***lue alas*** (engl. read-down) -ominaisuutena. Lue alas -ominaisuus määrittelee, että tietoa voidaan lukea vain alemman tason ja oman tason kerroksista. Käyttäjä s voi lukea kohdetta o, vain jos $S >= O$, missä S on käyttäjän s tietoturvataso ja O kohteen o tietoturvataso. [10, s. 137]

2. **-property* (*tähti-ominaisuus*), joka tunnetaan myös ***kirjoita ylös*** (engl. write-up) -ominaisuutena. Kirjoita ylös -ominaisuus määrittelee, että käyttäjä s voi kirjoittaa kohteeseen o, vain jos $O >= S$. Menetelmä estää käyttäjän tiedon kulkeutumasta muille tahoille kuin niille, jotka ovat korkeammalla tai samalla tasolla kuin käyttäjä. [10, s. 137]

Lue alas ja kirjoita ylös -ominaisuuksien mukainen tiedonkulku on kuvattu kuvaan 8.



Kuva 8: Bell-LaPadula -mallin mukainen tiedonkulku [16, s. 45]

BLP -mallin *kirjoita ylös* -ominaisuus yksinään ei ole riittävä suoja estämään tietojen vääristymistä ylemmillä tasoilla, millä käyttäjä on [10, s. 137]. Ominaisuus esimerkiksi mahdollistaa käyttäjän tasolla S ylikirjoittaa kohteita tasolla TS [16, s. 45]. Eheyden säilyttämiseksi ylemmillä tasoilla voidaan ongelma ratkaista muokkaamalla *kirjoita ylös* -ominaisuutta siten, että käyttäjä s voi kirjoittaa kohteeseen o, vain jos $S=O$ [10, s. 137].

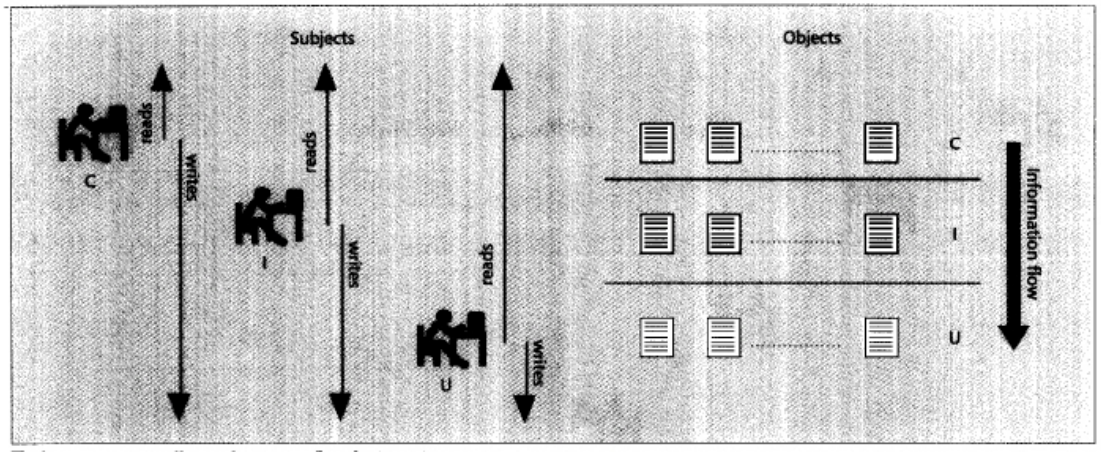
5.3.2 Biba -malli

Siinä missä BLP -malli pyrkii estämään luottamuksellisen tiedon kulkeutumisen epäluotetulle tasolle, Biba -malli pyrkii varmistamaan tiedon eheyden [10, s. 139]. Biba -malli seuraa samaa ideaa kuin BLP, eli tasojen tiedonkulkusuunta on määritelty säännöillä, mutta lähestyy ratkaisua eri suunnalta [10, s. 139]. Myös Biba -malli määrittelee tiedonkulun kahdella säännöllä [10, s. 139]:

1. *Simple-integrity property*, joka tunnetaan myös ***lue ylös*** (engl. read-up) -ominaisuutena. ***Lue ylös*** -ominaisuus määrittelee, että käyttäjä s voi lukea kohdetta o, vain jos $O >= S$. [10, s. 139] [16, s. 45]

2. *Integrity *-property*, joka tunnetaan myös ***kirjoita alas*** (engl. read-down) -ominaisuutena. ***Kirjoita alas*** -ominaisuus määrittelee, että käyttäjä s voi kirjoittaa kohteeseen o, vain jos $S >= O$. [10, s. 139] [16, s. 45]

Lue ylös ja *kirjoita alas* -ominaisuuksien mukainen tiedonkulku on kuvattu kuvaan 9. Biba -mallissa tasot kuvaavat eheyden tärkeyttä, eli kuinka paljon kohteen sisältämän tiedon sisältöön voidaan luottaa. Kuvan 9 tasot ovat Crucial (C), Important (I) ja Unknown (U). [16, s. 45]



Kuva 9: Biba -mallin mukainen tiedonkulku [16, s. 46]

Huomionarvoista on, että Biba -mallissa tiedonkulun suunta on vastainen BLP -malliin verrattaessa. Perinteisissä MAC -menetelmissä tiedonkulku on yksisuuntaista. [16, s. 45]

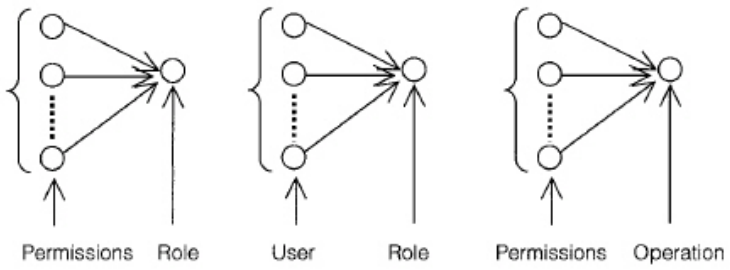
5.4 Roolipohjainen pääsynhallinta (RBAC)

Organisaatioissa pääsynhallintapäätökset perustuvat usein henkilöiden varsinaiseen työnkuvaan – rooliin – joka on heille määritelty. Tämä kattaa tehtävien, vastuualueiden ja valtuuksien erittelyn. Roolipohjaisen pääsynhallinta (engl. role-based access

control, RBAC) -menetelmän pääsynhallintapäätökset perustuvat juuri henkilöön kohdistuviin toimintoihin ja työnkuviin, joita hänen sallitaan suorittavan organisaatiossa. RBAC kehitettiin vaihtoehdoksi DAC ja MAC -menetelmille tarjoamaan sopivampi ja keskitetty ratkaisu teollisuuden ja siviilihallinnon tietoturvatarpeisiin. RBAC -menetelmän esittelivät ensimmäisen kerran Ferraiolo ja Kuhn vuonna 1992. [22]

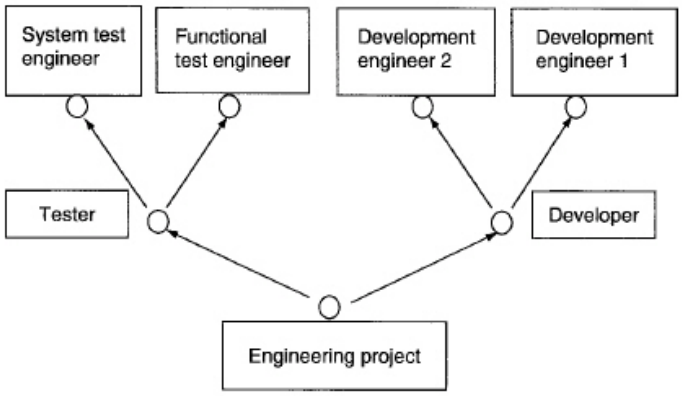
Toisin kuin DAC ja MAC -menetelmissä, joissa oikeudet on määritelty suoraan käyttäjille, RBAC -menetelmässä oikeudet on määritelty roolille [10, s. 26] ja rooli vuorostaan voidaan määritellä yhdelle tai usealle käyttäjälle [22]. RBAC -menetelmä mahdollistaa pääsynhallinnan suunnittelun abstraktimmalla tasolla, tehden hallintapolitiikasta neutraalimman kuin DAC ja MAC -menetelmissä [10, s. 26].

Rooli voidaan ajatella nippuna sallittuja valtuuksia, joita voidaan suorittaa organisaatiossa, tai rooli voidaan määritellä muodostuvan muista rooleista [22]. Tämä helpottaa roolien kuvaamista organisaation hierarkkisen rakenteen mukaan [10, s. 191]. Rooleihin määritellyt valtuudet voidaan edelleen määritellä varsinaisiksi järjestelmäkohtaisiksi käyttöoikeuksiksi, eli todellisiksi asetuksiksi joilla oikeus toteutetaan [10, s. 191]. Kuva 10 havainnollistaa valtuuksien, roolien, käyttäjien ja käyttöoikeuksien keskinäiset yhteydet.



Kuva 10: Valtuuksien, roolien, käyttäjien ja käyttöoikeuksien keskinäiset yhteydet [10, s. 192]

Kuva 11 havainnollistaa roolien hierarkkista muodostustapaa.



Kuva 11: Esimerkki yksinkertaisesta roolihierarkiasta (yhden roolin perintä) [10, s. 199]

5.4.1 Roolien määrittely ja hallinta

Roolien hallinta ja ylläpito voidaan määritellä kuuluvan osaksi pääsynhallintaprosessia ja pääsynhallintaprosessin tulee osaltaan huolehtia roolien sopivuudesta yrityksen toimintaan suorittamalla säännöllisiä tarkastuksia rooleihin. Vanhentuneet ja ei-toivotut roolit tulee poistaa. [1, s. 69]

Valtuudet rooleille määritellään joko järjestelmävalvojan toimesta [22], palvelun omistajan toimesta tai osana jatkuvaa pääsynhallintaprosessia [1, s. 69]. Roolin määritteleminen ei kuitenkaan ole kertaluonteinen tapahtuma, vaan niihin tulee tehdä tarkennuksia ja korjauksia säännöllisin väliajoin [25, s. 3]. Roolien määrittelystä käytetään kirjallisuudessa myös termiä *role engineering* [26].

Mitä enemmän rooleja on määritelty, sitä suuremmalla todennäköisyydellä roolien ristiriitaisuuksia ilmenee. Esimerkiksi jokin rooli sallii käyttäjän suorittaa tietyn toiminnon, kun taas toinen rooli kieltää tämän toiminnon suorittamisen. [1, s. 69] Lisäksi roolien suunnittelussa joudutaan aina miettimään, onko toimenpiteitä määritelty rooliin liian laajasti tai liian suppeasti [1, s. 69] Roolien ristiriitaisuuksia voidaan yrittää estää ja määrittelyn laajuutta kontrolloida roolien huolellisella suunnittelulla [1, s. 69], luvussa 3.1.1 mainitulla tehtävien eriyttämisellä sekä luvussa 3.1.2 mainitulla pienimmän oikeuden periaatteella.

Roolien määrittelylle on olemassa kaksi keskeistä lähestymistapaa: *Top-down* ja *bottom-up*. *Top-down* menetelmässä roolit määritellään pilkkomalla liiketoimintaprosessit pienemmiksi toiminnallisiksi yksiköiksi, joille kartoitetaan tarvittavat valtuudet. Toisin sanoen menetelmässä kuvataan yksittäiset työtehtävät rooleiksi määrittelemällä niille niiden tarvitsemat valtuudet. *Bottom-up* menetelmässä roolit kartoitetaan olemassa olevien oikeuksien perusteella. Menetelmän etuna on, että roolien määrittely voidaan osittain automatisoida. [27, s. 1]

6 Tapaustutkimus: Pääsynhallintamenetelmät IT-ulkoistuspalveluntarjoajayrityksessä

Tässä tapaustutkimuksessa selvitetään miten ja minkälaisilla menetelmillä pääsynhallinta on toteutettu Atos IT Solutions and Services Oy -yrityksessä. Tutkimuksen tarkoituksena on kartoittaa yrityksen pääsynhallinnan nykytila ja osoittaa siitä löydetyt ongelmakohdat sekä arvioida niiden vaikutukset yrityksen toimintaan.

Yrityksen pääsynhallinnan toteutuksen kartoitus aloitettiin selvittämällä, miten pääsynhallinta on palvelutoimintona yrityksessä määritelty ja minkälaisilla työkaluilla pääsynhallintaa toteutetaan. Käytetyt työkalut selvitettiin kysymällä esimiehiltä ja palveluiden omistajilta, miten uusille työntekijöille haetaan oikeuksia tietokohteisiin ja palveluihin, joita tarvitaan työn suorittamiseen. Työkalujen toimintatapaa selvitettiin lukemalla olemassa olevia dokumentaatioita ja ohjeita, tekemällä testitapauksia oikeuksienhausta ja haastattelemalla työntekijöitä. Toimintatavasta selvitettiin, mitä kohdejärjestelmiä niillä voidaan hakea ja minkälaista identiteetin- ja pääsynhallintamallia niissä noudatetaan.

Tapaustutkimuksessa selvitettiin myös, paljonko käyttöoikeuspyyntöjä työkalujen kautta kulkee, kauanko niiden läpivienti kestää ja kuinka paljon manuaalista työtä pyyntöihin sisältyy. Osa tiedoista saatiin työkaluista itsestään ja osa kerättiin haastatteluin ja tekemällä testikäyttöoikeuspyyntöjä. Havaintojen perusteella työkaluista koostettiin yhteenveto merkittävimmiksi koetuista ongelmakohdista. Lisäksi arvioitiin työkalujen soveltuvuutta yrityksen nykyiseen liiketoimintatapaan ja -tarpeisiin.

6.1 Pääsynhallinta palvelutoimintona ja käytetyt työkalut

Pääsynhallintaa ei ole yrityksessä määritelty itsenäiseksi palvelutoiminnoksi. Sen sijaan pääsynhallintaa toteutetaan kahden eri työkalun avulla: *Check In Request* (CIR) ja *Access Request Approval Process* (ARAP). Koska pääsynhallinta ei ole määritelty itsenäiseksi palvelutoiminnoksi, pääsynhallintaan liittyviä toimintoja ei ohjata tai valvota kenenkään toimesta eikä sille ole määritelty tarkasti vaatimuksia tietoturvan tai palvelun ylläpitämisen ja kehittämisen osalta.

Työkalut ARAP ja CIR eroavat toisistaan niin toiminnaltaan kuin sisällöltään. Työkaluista on tarjolla niukasti dokumentaatiota, mikä johtuu suurelta osin siitä, että molemmat työkalut ovat pitkälti yrityksen omiin tarpeisiin räätälöityjä.

6.1.1 Check In Request (CIR)

Check In Request (CIR) on *Lotus Notes Domino* -pohjainen käyttöoikeuksien hakemiseen tarkoitettu sovellus. Sovellus ei ole aktiivisesti kytketty kohdejärjestelmiin, eli se ei lue kohdejärjestelmistä niiden sisältämiä käyttöoikeuksia eikä se provisioi oikeuksia suoraan kohdejärjestelmiin. CIR ylläpitää tietoa käyttäjille sitä kautta haetuista ja hyväksytyistä valtuuksista, ja se on tarkoitettu vain yrityksen sisäiseen käyttöön.

CIR:lla haetaan oikeuksia pääasiallisesti yrityksen sisäisiin kohdejärjestelmiin, kuten tietokantoihin ja sovelluksiin, mutta sinne on mahdollista määrittää myös muita kohteita. Haettavat kohteet ovat luokiteltu kategorioihin ja näistä edelleen varsinaisiin käyttöoikeuskohteisiin. Riippuen kategoriasta, kohteet on kuvattu joko nimitasolla tai rooleina ja varsinaisen käyttöoikeuden laajuus ja tyyppi valitaan joko valintanapeista tai kirjoitetaan lisätiedot -kenttään. CIR:n käyttöliittymä on mukautettavissa usean erityyppisen käyttöoikeuskohteen mukaiseksi.

Käyttöoikeuskohteet on määritelty erilliseen sovellustietokantaan jota CIR lukee. Jokaiselle haettavalle kohteelle on määritelty pääkäyttäjä, joka toimii neljän silmän periaatteen mukaisesti yhtenä hyväksyjänä kohteeseen liittyvissä pyynnöissä. Pääkäyttäjän vastuu on myös määritellä ne todelliset käyttöoikeudet, jotka kohteeseen toteutetaan.

6.1.2 Access Request Approval Process (ARAP)

Access Request Approval Process (ARAP) on web-portaalin kautta toimiva käyttöoikeuksien hakemiseen tarkoitettu sovellus. Samoin kuin CIR, myöskään ARAP ei ole aktiivisesti kytketty kohdejärjestelmiin, eli se ei lue kohdejärjestelmistä niiden sisältämiä käyttöoikeuksia, eikä se provisioi oikeuksia suoraan kohdejärjestelmiin. ARAP ylläpitää tietoa käyttäjille sitä kautta haetuista ja hyväksytyistä valtuuksista.

ARAP:n kautta voidaan hakea oikeuksia yrityksen työntekijöille yrityksen omiin kohdejärjestelmiin ja yrityksen ylläpitämiin asiakasjärjestelmiin. Vaikka palvelu on mahdollista tarjota myös yrityksen ulkopuolisille tahoille, on päätetty, että vain yrityksen sisäiset työntekijät voivat luoda ARAP:n kautta pyyntöjä. ARAP myös mahdollistaa ulkopuolisten hyväksyjien käytön, jolloin hyväksyntäketjussa voidaan tarvittaessa käyttää asiakkaan yhteyshenkilöä.

ARAP:n kautta haettavista kohdejärjestelmistä ei löytynyt olemassa olevaa dokumentaatiota. Työkalun käyttämää kohdejärjestelmätietokantaa tutkimalla onnistuttiin työstämään kattava listaus ARAP:n kautta haettavista kohdejärjestelmistä ja listauksen ylläpito siirrettiin työkalun ylläpitäjän vastuulle. Lisäksi tutkimuksen ohella tehtiin ohjeistus organisaation työntekijöille, jossa kerrottiin, mitä oikeuksia

ARAP:n kautta on tarkoitus hakea ja miten ne eroavat CIR:stä.

Pääpiirteittäin ARAP:n kautta on mahdollista hakea seuraavanlaisia oikeuksia:

- Kaikki domain admin oikeudet yrityksen kohdejärjestelmiin
- Kaikki domain admin oikeudet ylläpidettyihin asiakasjärjestelmiin
- Kulkuluvat palvelinhuoneisiin

Haettavia käyttöoikeuskohteita ylläpidetään erillisessä *Hardware Info* tietokannassa ja tietojen ylläpidosta vastaa yrityksen *Configuration Management* yksikkö. *Hardware Info* on manuaalisesti ylläpidetty tietokanta ja muutokset sinne on määritelty tehtäväksi osana *Change* ja *Configuration Management* prosesseja.

Kohteet on ryhmitelty asiakkaittain ja tämän jälkeen palvelu-/tuotantojärjestelmien perusteella. Tietokanta mahdollistaa teknisen- ja yrityshyväksyjän asettamisen jokaiselle kohteelle yksitellen. Tietokanta ei tue kohteiden etsintää nimillä, vaan ARAP pyynnön tekijän tulee tietää tai osata etsiä oikea kohde asiakkuuden palvelu- tai tuotantojärjestelmien alta.

6.2 Identiteetinhallintamenetelmät

CIR ei ylläpidä itsessään käyttäjien identiteettejä eikä täten toteuta identiteetinhallintaa sellaisenaan. Käyttäjätiedot luetaan suoraan HR:n ylläpitämästä *Citizen* henkilötietokannasta. CIR:n kautta ei voida muokata identiteettejä. CIR tallentaa omaan tietokantaansa tiedon sitä kautta käyttäjille haetuista ja hyväksytyistä valtuuksista.

Citizen toimii luvussa 4.1 esitellyn jaetun paikallisen identiteetin mallin mukaisesti, eli useampi järjestelmä voi lukea sen ylläpitämän käyttäjärekisterin tietoja. Käyttäjälle, jonka henkilötietoja ei ole *Citizen* tietokannassa, ei voida hakea CIR:n kautta oikeuksia. Tämä rajaa CIR käyttäjäkunnan yrityksen sisäisiin työntekijöihin ja niihin kolmansiin osapuoliin tai globaalin organisaation sisäisiin partnereihin, jotka on kirjattu *Citizen* tietokantaan.

ARAP ylläpitää omaa paikallisen identiteetin mallin mukaista käyttäjärekisteriä, eikä se ole kytköksissä yrityksen HR järjestelmään. ARAP:n ylläpitämä käyttäjärekisteri on jaettu saman portaalin kautta toimivan, muutospyynnöille tarkoitetun CMweb (*Change Management web*) konsolin kanssa.

ARAP:n identiteetin hallinnan yhdeksi ongelmakohdaksi havaittiin, että käyttäjärekisteri ei osaa poistaa vanhentuneita käyttäjätilejä automaattisesti, vaan poistot tulee tehdä järjestelmän ylläpitäjän toimesta manuaalisesti. Lisäksi tiliin liitetyt oikeudet tulee pyytää poistettaviksi erikseen.

Pääsynhallintatyökaluihin liittyvien identiteettien lisäksi yrityksessä on käytössä verkkoidentiteetit työntekijälle, joita hallinnoidaan *Microsoft Active Directoryn* avulla. *Active Directory* sisältää tiedon verkon käyttäjistä ja resursseista, ja mahdollistaa resurssien jakamisen käyttäjille luvussa 4.2 esitellyn verkkoidentiteetin mallin mukaisesti. Sekä ARAP:lla että CIR:llä voidaan hakea verkkoidentiteeteille pääsyoikeuksia valittuihin verkon resursseihin.

6.3 Pääsynhallintamenetelmät

CIR:n toimintatapa noudattaa perusperiaatteeltaan luvussa 5.2 esitellyn suljetun harkinnanvaraisen pääsynhallintamallin (DAC) toimintatapaa. Pääsy kohdejärjestelmiin toteutetaan perustuen käyttäjän identiteettiin ja siihen liitettyihin valtuuksiin, lisäksi kaikille haettaville kohdejärjestelmille on määritelty pääkäyttäjä. CIR toimii pitkälti luvussa 5.2 esitellyn reference monitorin tavoin, jota vasten voidaan tarkastaa, saako henkilöllä olla tietyt oikeudet järjestelmiin.

Erona varsinaiseen määritelmään DAC:sta CIR:n toimintatavassa pääkäyttäjä ei itse luo varsinaisia oikeuksia kohdejärjestelmään, vaan toimii ainoastaan yhtenä hyväksyjänä pyynnöille. Oikeuksienhaussa noudatetaan luvussa 3.1.1 esitellyn tehtävien eriyttämisen (SoD) mukaista tietoturvapolitiikkaa toimimalla yrityksen tietoturvahallinnan määrittelemän neljän silmän periaatteen mukaisesti. Jokaiseen pyyntöön tarvitaan kaksi hyväksyjää: esimies ja pääkäyttäjä. Tämä estää tilanteen, jossa käyttäjä voisi hakea ja hyväksyä oikeuden itselleen, jossa toimii pääkäyttäjänä. Lisäksi jos esimies ja pääkäyttäjä ovat yksi ja sama henkilö, asetetaan esimiehen esimies toiseksi hyväksyjäksi automaattisesti.

Samoin kuin CIR myös ARAP:n toimintatapa noudattaa perusperiaatteeltaan luvussa 5.2 esitellyn suljetun harkinnanvaraisen pääsynhallinnan mallia (DAC). Pääsy kohdejärjestelmiin toteutetaan perustuen käyttäjän identiteettiin ja siihen liitettyihin valtuuksiin. ARAP ei mahdollista pääkäyttäjien määrittämistä kohdejärjestelmille, mutta mahdollistaa teknisten- ja yrityshyväksyjien asettamisen kohdejärjestelmille. Myös ARAP toimii luvussa 5.2 esitellyn reference monitorin tavoin. Sitä vasten tarkistetaan, saako henkilöllä olla tietyt oikeudet järjestelmiin.

ARAP:n pääsynhallinnassa pyritään myös noudattamaan tehtävien eriyttämistä (SoD) neljän silmän periaatteen avulla siten, että jokaiseen pyyntöön vaaditaan vähintään kaksi hyväksyjää: esimies ja tekninen hyväksyjä tai mahdollinen yrityshyväksyjä. SoD on kuitenkin mahdollista kiertää ja sitä on mahdollista manipuloida. Jokainen avattu pyyntö tarvitsee tarkistaa ja lähettää eteenpäin pääsynhallintakoordinaattorin toimesta ennen hyväksyntää. Pääsynhallintakoordinaattori asettaa pyynnölle hyväksyjät. Tämä mahdollistaa kaikkien pääsynhallintakoordinaattorioikeuksien omaavien henkilöiden pystyvän tekemään, sekä hyväksymään, itselleen mitä tahansa käyttöoikeuksia.

6.4 Prosessi ja osapuolet

Käyttoikeuspyyntöjen käsittely ja toteutus CIR:lla kartoitettiin tekemällä viisi testikäyttöoikeuspyyntöjä ja haastattelemalla kahta työkalun aikaisempaa kehittäjää. Haastattelut olivat vapaamuotoisia ja testikäyttöoikeuspyynnöt rajoittuivat yrityksen *SharePoint* ympäristön kohteisiin. Saaduista tuloksista CIR:n toimintatapa kuvattiin prosessiksi, joka koostuu viidestä vaiheesta:

1. **Pyynnön avaus ja määrittely.** Käyttöoikeuspyyntö avataan CIR:iin ja siihen määritellään mitä oikeutta haetaan, kenelle haetaan ja miksi haetaan. Oikeuspyynnön voi avata kuka tahansa yrityksen sisäinen työntekijä.

2. **Hyväksyntä.** Käyttöoikeuspyyntö ohjautuu CIR:iin asetettujen tietojen mukaisesti hyväksyttäväksi ensin oikeuden saajan esimiehelle ja tämän jälkeen haettavaan oikeuteen liittyvän kohdejärjestelmän pääkäyttäjälle. Hyväksynnän jälkeen CIR tallentaa tietokantaansa tiedon, että käyttäjällä on valtuus haettuun oikeuteen.

3. **Koordinointi.** CIR luo käyttöoikeuspyynnöstä sähköpostin yrityksen *Service Deskiin*, joka tulkitsee sen ja luo siitä palvelupyynnön tiketöintijärjestelmään. Palvelupyyntö ohjautuu tiketöintijärjestelmästä oikeuden toteutuksesta vastaavalle tuotantotiimille.

4. **Toteutus.** Tuotantotiimi tulkitsee palvelupyynnössä pyydetyn käyttöoikeuden tiedot ja toteuttaa ne kohdejärjestelmään. Tuotantotiimi on vastuussa myös toteutuksen tiedottamisesta pyynnön luojalle ja oikeuden saajalle.

5. **Sulkeminen.** Tuotantotiimi ilmoittaa oikeuden saajalle oikeuden toteutuksesta ja tämän jälkeen tuotantotiimi sulkee palvelupyynnön tiketöintijärjestelmästä.

Vastaavasti ARAP:n käyttöoikeuspyyntöjen käsittelyyn ja toteutukseen tutustuttiin tekemällä viisi testikäyttöoikeuspyyntöjä ja haastattelemalla yhtä prosessikoordinaattoria. Testikäyttöoikeuspyynnöt rajoittuivat yrityksen testiympäristöjen oikeuskohteisiin. Haastattelu oli vapaamuotoinen. Lisäksi tutustuttiin työkalusta luotuun käyttöoppaaseen. Näiden perusteella työkalun toimintatavasta tehtiin prosessikuvaus, joka koostuu kuvan 12 mukaisesti viidestä vaiheesta. Kuva 12 tehtiin, englanniksi, sillä kohdeyrityksen työkielenä käytetään englantia.

Kuva 12: Käyttöoikeuspyyntöjen käsittelyn vaiheet ARAP:ssa

1. **Määrittely.** Käyttöoikeuspyyntö avataan ARAP:iin ja siihen määritellään mitä oikeutta haetaan, kenelle haetaan ja miksi haetaan. Käyttöoikeuspyynnön voi avata kuka tahansa yrityksen sisäinen työntekijä.

2. **Koordinointi.** Pääsynhallintakoordinaattori tarkistaa käyttöoikeuspyynnön sisällön ja pyytää siihen tarvittaessa tarkennuksia ja korjauksia oikeuden avaajalta. Koordinaattori myös tarkistaa ja tarvittaessa lisää oikeat hyväksyjät pyynnölle ja tämän jälkeen lähettää pyynnön hyväksyjille hyväksyttäväksi.

3. **Hyväksyntä.** Käyttöoikeuspyynnöstä ohjautuu sähköpostiviesti asetetuille hyväksyjille. Hyväksyjien tulee tarkastaa pyyntö ja joko hyväksyä tai hylätä se. Kun pyyntö on hyväksytty, pääsynhallintakoordinaattori luo pyynnön perusteella palvelupyynnön yrityksen tiketöintijärjestelmään.

4. **Toteutus.** Tuotantotiimi tulkitsee palvelupyynnössä pyydetyn käyttöoikeuden tiedot ja toteuttaa ne kohdejärjestelmään.

5. **Sulkeminen.** Tuotantotiimi on vastuussa sulkemisista. ARAP lähettää oikeuden saajalle viestin oikeuden toteutumisesta sulkemisen tapahtuessa. ARAP:n tietokantaan jää tieto käyttäjälle haetusta ja toteutetusta oikeudesta.

6.5 Pyyntöjen määrät, läpivientiaika ja käytetty aika

CIR:n kautta tehdyt käyttöoikeuspyynnöt tallentuvat CIR:n ylläpitämään tietokantaan haetuista oikeuksista. CIR:n kautta haettavat oikeudet lajiteltiin *Sharepoint* pyyntöihin ja muihin pyyntöihin, sillä *Sharepoint* pyyntöjä on CIR:n kautta haettavista oikeuksista yli puolet. Oikeuden saaminen *Sharepointtiin* on usein hyvin oleellista työtehtävien suorittamisen mahdollistamiseksi.

ARAP:n kautta tehdyt käyttöoikeuspyynnöt tallentuvat ARAP:n ylläpitämään tietokantaan. Tietokannasta saatiin selville pyyntöjen määrät, mutta tietokanta ei kuitenkaan sisällä tietoa kauanko pyynnön eri vaiheisiin on kulunut aikaa eikä tietoa kauanko pyyntöihin on käytetty aikaa käyttäjien toimesta.

6.5.1 Pyyntöjen määrät

Pyyntöjen määriä tarkasteltiin neljän kuukauden jaksolta, josta otettiin keskiarvo kuvaamaan kuukausittaista volyymia. CIR:n osalta tarkasteltujen käyttöoikeuspyyntöjen määrät ja keskiarvot löytyvät taulukosta 1.

Taulukko 1: Käyttöoikeuspyyntöjen määrät CIR:ssä.

	Neljän kuukauden kokonaismäärä	Kuukausittainen keskiarvovolyymi
SharePoint pyynnöt	303	76
Tiketöintityökalusta haetut muut CIR:ssä luodut käyttöoikeuspyynnöt	292	73
Kokonaismäärä:	595	149

ARAP:n kautta kulkevien käyttöoikeuspyyntöjen määrät saatiin siirtämällä tietokannan tiedot taulukkolaskentaohjelmaan. Myös ARAP pyyntöjen määriä tarkasteltiin neljän kuukauden jaksolta, josta laskettiin kuukausittainen keskiarvovolyymi. ARAP:n osalta tarkasteltujen käyttöoikeuspyyntöjen määrät ja keskiarvo löytyvät taulukosta 2.

Taulukko 2: Käyttöoikeuspyyntöjen määrät ARAP:ssä.

	Neljän kuukauden kokonaismäärä	Kuukausittainen keskiarvovolyymi
Määrä	436	109

6.5.2 Pyyntöjen läpivientiaika

Läpivientiaikojen tarkastelussa tilannetta hankaloitti se, että CIR:stä ei saatu tietoa ulos taulukkomuotoisesti, vaan pyyntöjä täytyi tarkastella työkalusta käsin yksi kerrallaan. Läpivientiaikoja ei myöskään voitu vahvistaa muiden kuin *Sharepoint* pyyntöjen osalta, sillä tiketöintityökalun aikaleimat antavat vain toteutumisesta sulkeutumiseen kuluvan ajan. Haastatteluilla kerätyistä tiedoista ja käyttäjien kokemuksista voidaan kuitenkin olettaa, että muiden käyttöoikeuspyyntöjen läpivientiajat ovat samansuuntaisia kuin *Sharepoint* pyyntöjen.

Pyyntöjen läpivientiajoista CIR:ssa löydettiin suurta vaihtelua; jotkin pyynnöt saattoivat toteutua päivän sisällä ja jotkin saattoivat kestää jopa kuukausia. Läpivientiaikojen ääripäitä edustavien pyyntöjen määrän arvioitiin olevan 20 % kaikista pyynnöistä, perustuen työkalusta tarkistettuihin pyyntöihin. Tarkastelusta jätettiin pois läpivientiaikojen räikeät ääripäät ja tarkastelu suoritettiin vain rajatulle määrälle pyyntöjä.

Pyyntöjen läpivientiaikaa CIR:ssa tarkasteltiin siitä hetkestä, kun pyyntö on luotu järjestelmään, siihen, kun se on kuitattu toteutetuksi. Vain toteutuneet pyynnöt

otettiin tarkasteluun. Taulukossa 3 on CIR pyyntöjen keskimääräiset ajat jaoteltuna kolmeen osaan: 1) avaamisesta hyväksymiseen kulunut aika, 2) hyväksynnästä sulkeutumiseen kulunut aika ja 3) kokonaisläpivientiaika. Näistä ajoista kokonaisläpivientiaika on loppukäyttäjän kokema aika.

Taulukko 3: Pyyntöjen läpivienti ajat CIR:ssä.

	Avaamisesta hyväksymiseen kulunut aika	Hyväksymisestä sulkeutumiseen kulunut aika	Kokonaisläpivientiaika
Keskiarvo tunteina	129	130	260
Keskiarvo kalenteripäivinä	5,4	5,4	10,8

ARAP pyyntöjen läpivientiaikojen tarkasteltiin tekemällä kymmenen testikäyttöoikeuspyyntöä ja haastattelemalla neljää oikeuden saajia ja yhtä pääsynhallintakoordinaattoria. Testikäyttöoikeuspyyntöihin ja haastatteluihin perustuen koostettiin taulukon 4 mukaiset arviot pyynnön elinkaaren eri vaiheiden viemästä ajasta ja kokonaisläpivientiajasta.

Taulukko 4: Pyyntöjen läpivienti ajat ARAP:ssa.

	Määrittelystä hyväksyntävaiheeseen kulunut aika	Hyväksynnästä toteuttamisvaiheeseen kulunut aika	Toteuttamisesta sulkeutumiseen kulunut aika	Kokonaisläpivientiaika
Arvio tunteina	24	120	48	192
Päivinä	1	5	2	8

6.5.3 Pyyntöihin käytetty aika

Pyyntöihin käytetty aika arvioitiin haastattelujen perusteella. Haastateltavat antoivat arvion pyyntöön keskimäärin käyttämästään ajasta. Haastattelut kohdistuivat sellaisiin käyttäjiin, jotka luovat pyyntöjä, ja käyttäjiin, jotka hyväksyvät pyyntöjä. Haastattelut olivat luonteeltaan avoimia, joissa haastateltavat saivat kertoa omin sanoin mitä toimintoja tekevät käyttöoikeuspyyntöihin liittyen ja kauanko aikaa niihin kuluu.

Pyynnön luomiseen käytetty aika arvioitiin siitä hetkestä, kun käyttäjä avaa työkalun, siihen hetkeen, kun hän on täyttänyt tarvittavat tiedot pyyntöön ja tallentanut sen. Samoin hyväksyntään käytetty aika arvioitiin siitä hetkestä, kun hyväksyjä avaa työkalun, siihen hetkeen, kun hyväksyjä painaa hyväksyntä painiketta. Toteuttamiseen käytettyä aikaa arvioidaan työn myöhemmässä osiossa 6.6 Pyyntöjen toteutus. Pyyntöihin käytetyt ajat koskevat sekä CIR:n että ARAP:n kautta luotuja pyyntöjä, ellei toisin mainita.

Pyynnön luomisen osalta haastateltiin viittä työntekijää, joista kolme oli esimiesasemassa ja kaksi tuotantotiimin asiantuntijoita. Pyynnön luomiseen arvioitiin käytettävän keskimäärin 15 minuuttia, josta suurin osa kuluu kohdejärjestelmän etsimiseen listasta. Hyväksynnän osalta haastateltiin viittä työntekijää, joista kolme oli sekä esimiehiä että palvelunomistajia ja kaksi työkalun/palvelun omistajia. Hyväksyntään hyväksyjät arvioivat käyttävänsä keskimäärin 5 minuuttia, josta suurin osa kuluu pyynnön tarpeellisuuden arvioimiseen. Neljän silmän periaatteen mukaisesti hyväksyjiä on aina kaksi, jolloin kokonaisaika hyväksyjien osalta on 10 minuuttia. ARAP:n osalta haastateltiin vielä pääsynhallintakoordinaattoria, joka arvioi käyttävänsä yhden oikeuspyynnön käsittelyyn sen elinkaaren aikana keskimäärin 15 minuuttia.

CIR:n osalta osapuolten yhteenlaskettu yhteen pyyntöön käyttämä työaika on 25 minuuttia. ARAP:n osalta osapuolen yhteenlaskettu yhteen pyyntöön käyttämä työaika on 40 minuuttia.

6.6 Pyyntöjen toteutus

Sekä CIR:n että ARAP:n kautta pyydettyjen käyttöoikeuksien varsinainen toteutus tehdään asiantuntijatiimeissä. Tieto tiimeille tulee tiketöintityökalun kautta palvelupyyntöinä. Taulukoista 3 ja 4 löytyvät arviot siitä, kauanko hyväksymisestä sulkemiseen menee aikaa tai kauanko toteuttamiseen menee aikaa. Nämä ajat kuvaavat aikaa, jonka pyyntö on tiketöintityökalussa.

Varsinainen oikeuden toteutukseen käytetty aika selvitettiin haastattelemalla tiimien asiantuntijoita. Kävi ilmi, että oikeuksien toteutuksen vaatima varsinainen työmäärä on varsin pieni. Haastateltavat arvioivat kokonaisajaksi yhtä pyyntöä kohden kuluvan keskimäärin 15 minuuttia.

Jos verrataan CIR:n läpivientiajassa mainittua hyväksymisestä sulkeutumiseen kulunutta aikaa (130 h) ja ARAP:n läpivientiajassa mainittua toteuttamisessa kulunutta aikaa (48 h) varsinaiseen työn toteuttamiseen käytettyyn aikaan (15 min), huomataan, että ero on erittäin suuri. Aikaerot on kuitenkin helppo perustella. CIR:n tapauksessa aikaa kuluu siihen, että hyväksynnän jälkeen pyyntö lähtee työkalusta sähköpostina *Service Desk*:iin. *Service Desk* avaa sähköpostin, tulkitsee sen ja luo sen perusteella palvelupyynnön tiketöintijärjestelmään. Palvelupyyntö ohjautuu

asiantuntijatiimin jonoon odottamaan ja vasta jonosta se valitaan toteutettavaksi. Vastaavasti ARAP:n tapauksessa hyväksynnän jälkeen pääsynhallintakoordinaattori luo palvelupyynnön tiketöintijärjestelmään, jossa se ohjautuu asiantuntijatiimin jonoon odottamaan ja vasta jonosta se valitaan toteutettavaksi.

Tuloksista voidaan todeta, että pyyntöjen toteuttamisajasta suurin osa menee odottamiseen *Service Deskin* sähköpostissa, pyynnön tulkitsemiseen ja muuttamiseen palvelupyynnöksi tiketöintijärjestelmään sekä jonottamiseen tiketöintijärjestelmässä tuotantotiimin jonossa. Itse oikeuden toteutus vie vain pienen osan koko toteuttamisajasta.

6.7 Havaitut ongelmakohdat työkaluissa

Työkalujen toiminnallisuutta, läpivientiaikoja ja käyttäjähaastattelujen tuloksia tutkimalla tehtiin yhteenveto merkittäviksi koetuista ongelmakohdista. Ongelmakohtien perusteella tutkimuksessa tehtiin lyhyt arvio ongelmakohdan toiminnallisesta seurauksesta. Lisäksi arvioitiin mahdollinen liiketoiminnallinen vaikutus, jonka tarkoitus on helpottaa ongelmakohtien priorisointia yrityksessä myöhemmin. Lisäksi huomattiin, että ongelmat ovat luonteeltaan joko yrityksen resursseja tuhlaavia, tietoturvaa uhkaavia tai molempia. Taulukko 5 sisältää CIR:stä kerätyt ongelmakohdas ja taulukko 6 ARAP:sta kerätyt ongelmakohdat.

Taulukko 5: Havaitut ongelmakohdat CIR:ssa

No.	Ongelmakohta	Toiminnallinen seuraus	Liiketoiminnallinen vaikutus	Luonne (R=resursseja tuhlaava, T=tietoturvaa uhkaava)
1	Ei mahdollisuutta luoda sääntöihin tai automaatioon perustuvaa käyttöoikeuksien jakamista.	Kaikki oikeudet, joita käyttäjät tarvitsevat työnsä tekemiseen, tulee hakea manuaalisesti jonkin henkilön toimesta.	Työaikaa kuluu sellaisten käyttöoikeuksien hakemiseen, jotka voitaisiin mahdollisesti mallintaa roolimalleihin ja/tai automatisoida.	R
2	Vain yhdelle henkilölle kerrallaan voidaan hakea oikeuksia.	Kaikille samoissa työtehtävissä/rooleissa työskenteleville henkilöille tulee tehdä samat käyttöoikeuspyynnöt.	Työaikaa kuluu, kun tarvitsee tehdä samat käyttöoikeuspyynnöt usealle henkilölle vaikka he suorittavat samoja työtehtäviä/roolia.	R
3	Vain yksi oikeus kerrallaan voidaan hakea oikeuksia.	Jokainen käyttöoikeuspyyntö tarvitsee avata erikseen.	Työaikaa kuluu, kun jokainen käyttöoikeuspyyntö tarvitsee avata erikseen.	R
4	Käyttäjät eivät löydä haluamaansa käyttöoikeuskohdetta	Käyttäjällä kuluu aikaa. Pääsynhallintaprosessi saatetaan "ohittaa"suoralla palvelupyynnöllä tiketöintijärjestelmään. Puuttuvasta käyttöoikeuskohteesta ei ilmoiteta kenellekkään.	Työaikaa kuluu. Tietoturvariskit kasvavat jos kirjanpito jaetuista käyttöoikeuksista on puutteellista.	R & T
5	Käyttöoikeuksien toteutumisen koetaan olevan hidasta.	Oikeuden saaja joutuu odottamaan ja ei pysty suorittamaan työtehtäviään järjestelmien osalta, joihin tarvitaan käyttöoikeutta.	Työaikaa kuluu.	R
6	Organisaatioyksikköihin perustuvan roolitietokannan ylläpito CIR:ssa ei mahdollista.	Palveluiden omistajat ja yksiköiden esimiehet joutuvat itse säilyttämään tietoa yksilölle tarpeellisista käyttöoikeuksista.	Ei yhtenäistä prosessia tai ohjetta yksikkökohtaisten roolitietojen ylläpitoon, jolloin tehtävien eriyttämistä ja pienimmän oikeuden tietoturvaperiaatetta on vaikea noudattaa ja valvoa.	T

Taulukko 6: Havaitut ongelmakohdat ARAP:ssa.

No.	Ongelmakohta	Toiminnallinen seuraus	Liiketoiminnallinen vaikutus	Luonne (R=resursseja tuhlaava, T=tietoturvaa uhkaava)
1	Ei sääntöihin tai automaatioon perustuvaa käyttöoikeuksien jakamista.	Kaikki oikeudet tulee hakea manuaalisesti jonkin henkilön toimesta.	Työaikaa kuluu käyttöoikeuksiin, jotka voitaisiin mallintaa roolimalleihin ja automatisoida.	R
2	Vain yhdelle henkilölle kerrallaan voidaan hakea oikeuksia.	Kaikille samoissa työtehtävissä työskenteleville henkilöille tehdään käyttöoikeuspyynnöt yksittäin.	Työaikaa kuluu, vaikka samat pyynnöt usealle henkilölle.	R
3	Käyttäjärekisteri ei automaattisesti poista vanhentuneita käyttäjätilejä.	Järjestelmän ylläpitäjän tulee poistaa vanhentuneet käyttäjätilit manuaalisesti.	Työaikaa kuluu poistoihin. Tietoturvariskit kasvavat, jos henkilötiedot jostain syystä jäävät poistamatta.	R & T
4	Tehtävien eriyttäminen (SoD) mahdollista kiertää.	Käyttöoikeuksien hakemiseen suunniteltua prosessia ohitetaan hyväksynnän osalta.	Yrityksen tietoturva voi olla uhattuna, jos koordinaattorioikeudet joutuvat vääriin käsiin.	T
5	Haettavan kohteen löytäminen vaikeaa.	Käyttäjällä kuluu aikaa. Pääsynhallintaprosessi saatetaan ohittaa palvelupyynnöllä tiketöintijärjestelmään.	Työaikaa kuluu. Tietoturvariskit kasvavat jos kirjanpito jaetuista käyttöoikeuksista on puutteellista.	R & T
6	Pyynnön toteutuminen on hidasta.	Oikeuden saaja joutuu odottamaan ja ei pysty suorittamaan työtehtäviään.	Työaikaa kuluu.	R
7	Organisaatioyksikköihin perustuvan roolitietokannan ylläpito ei mahdollista.	Käyttöoikeuksien hakeminen työtehtävien muuttuessa työlästä.	Puutteelliset kuvaukset organisaatioyksiköiden oikeuksista.	T

6.8 Yhteenveto tapaustutkimuksesta

Tapaustutkimus paljastaa, että yrityksen pääsynhallinta on osittain puutteellisesti toteutettu, sillä pääsynhallintaa ei ole määritelty yrityksessä palvelutoiminnoksi eikä pääsynhallintaa johdeta minkään palvelukokonaisuuden toimesta. Lisäksi yhteisen toimintatavan kuvauksessa on suuria puutteita, eikä työntekijöille ole aina selvää, miten pääsyoikeuksia tulee yrityksessä hakea.

CIR:n ei koeta pystyvän vastaamaan yrityksen tämän hetkisiin liiketoimintatapaan ja -tarpeisiin. Saadut tulokset työkalusta tukevat koettua käsitystä. CIR on aikanaan toteutettu yrityksen sisäisten sovellusten hallintaan, mutta se ei kunnolla pysty vastaamaan palvelutuotannon tarpeisiin. Skaalautuvuus on yksi isoimmista ongelmakohdista, sillä nykyään ylläpidettävien järjestelmien määrä on suuri ja niihin kohdistuu paljon muutoksia tiheällä aikavälillä. Myös käyttäjäkunta on monimuotoisempaa kuin aikaisemmin, esimerkiksi ulkoisten työntekijöiden määrä on kasvanut ja vaihtuvuus lisääntynyt. Työkalu ei tue sääntöihin perustuvaa oikeuksien jakoa tai mahdollista automatisointia. Lisäksi roolitietokannan ja rooleihin perustuvan pääsynhallinnan toteuttaminen työkalussa ei ole mahdollista tai ainakin hyvin hankalaa. Pyynnön läpivientiajasta suurin osa menee muuhun kuin varsinaiseen oikeuden toteuttamiseen.

Samoin kuin CIR:n, myöskään ARAP:n ei koeta pystyvän vastaamaan yrityksen tämän hetkisiin liiketoimintatapaan ja -tarpeisiin. Saadut tulokset työkalusta tukevat koettua käsitystä. Myös ARAP:n yksi isoimmista ongelmista on skaalautuvuus, sillä henkilö- ja laiterekisteritietokannan hallinta ei kykene vastaamaan organisaatiossa tapahtuviin muutoksiin riittävän nopeasti ja tarkasti. Pyynnön läpivientiajasta suurin osa menee muuhun kuin varsinaiseen oikeuden toteuttamiseen. Työkalu ei tue sääntöihin perustuvaa oikeuksien jakoa tai mahdollista automatisointia, eikä roolitietokannan ja rooleihin perustuvan pääsynhallinnan toteuttamista. Lisäksi työkalussa on tietoturvapuutteita, joista suurimmaksi nousee SoD:n kiertomahdollisuus.

7 Pääsynhallinnan toteutusehdotus

Tässä kappaleessa esitellyn toteutusehdotuksen tarkoituksena on tarjota kattava kokonaiskuvaus siitä, miten pääsynhallinta voitaisiin Atos IT Solution and Services Oy -yrityksessä toteuttaa. Tavoitteena on kuvata pääsynhallinta siten, että se voitaisiin määrittää yrityksen yhdeksi palvelutoiminnoista ja että se lisäisi osaltaan yrityksen tietoturvaa ja tehostaisi käyttöoikeuspyyntöjen hallintaa ja toteutusta. Esitellyt toteutusehdotukset ja kuvaukset on tehty osana diplomityötä perustuen teoriaosuudessa esiteltyihin ratkaisuihin ja käytäntöihin siten, että ne soveltuvat Atos IT Solutions and Services yrityksen tarpeisiin. Kaikkien esiteltyjen kuvien tekstit ovat englanniksi, sillä kuvat luotiin yrityksen käyttöön ja yrityksen työkielenä käytetään englantia. Kaikki esitellyt taulukot on diplomityössä esitelty suomeksi.

IT-ulkoistuspalveluita tarjoavan yrityksen toimintaan soveltuvan pääsynhallinnan toteutusta lähdettiin suunnittelemaan laatimalla vaatimusmäärittely toteutukselle. Vaatimusmäärittely laadittiin, jotta saataisiin kehys ratkaisun tavoitteista ja vaatimuksista, sekä kuvaus, miten ratkaisun tulisi toimia ja millä keinoilla toiminnallisuudet saavutetaan. Vaatimusmäärittelyn sisältämien asioiden lisäksi toteutusta suunniteltiin luvussa 1.3 esiteltyjä arviointikriteereitä silmällä pitäen.

Pääsynhallinta määriteltiin olevan yksi palvelutoiminnoista IT palveluorganisaatiossa. Sen toiminta kuvattiin prosessiksi sisältäen myös vastuualueiden määrittelyt. Pääsynhallintamenetelmäksi valittiin luvussa 5.4 esitelty roolipohjainen pääsynhallinta, tukien kuitenkin luvussa 5.2 esitellyn harkinnanvaraista pääsynhallinnan mukaista toimintatapaa, jossa kohdejärjestelmille on määritelty pääkäyttäjä.

Teknistä toteutusta varten pääsynhallinnalle oli ennalta valittu työkalu, jolla yrityksen pääsynhallinta suunniteltiin toteutettavan. Työkalulle ei kuitenkaan ollut määritelty toiminnallisia vaatimuksia, rajapintakuvauksia eikä provisiointiratkaisuja, jotka ovat pakollisia työkalun konfiguroimisen ja käyttöönoton kannalta. Työkalulle tehtiin toiminnallinen vaatimusmäärittely ja havainnekuva, jolla pyrittiin kuvaamaan toiminnallisuuden kannalta oleelliset toiminnot ja rajapinnat. Lisäksi määriteltiin käyttöoikeuksien provisiointiratkaisut ja arvioitiin työkalun soveltuvuutta niiden toteuttamiseen.

7.1 Toteutuksen vaatimusmäärittely

Osana diplomityötä pääsynhallinnan toteutuksehdotukselle tehtiin vaatimusmäärittely. Vaatimusmäärittely perustuu yrityksen tarpeeseen tarjota keskitettyä pääsynhallintaa tietoturvallisesti suurelle määrälle käyttäjiä, ottaen huomioon kohdejärjestelmiin kohdistuvien muutosten tiheys. Lisäksi otettiin huomioon nykyisistä työkaluista havaitut ongelmakohdat, joiden koettiin oleellisesti uhkaavan tietoturvaa tai hidastavan pääsynhallintaprosessia. Vaatimuksille määriteltiin nimi, kuvaus ja prioriteetit. Vaatimusmäärittelyllä asetettiin yleiset reunaehdot, jotka valitun toteu-

tusratkaisun tulee toteuttaa. Vaatimusten prioriteettien nimien lyhenteen ja niiden kuvaukset on löytyvät taulukosta 7.

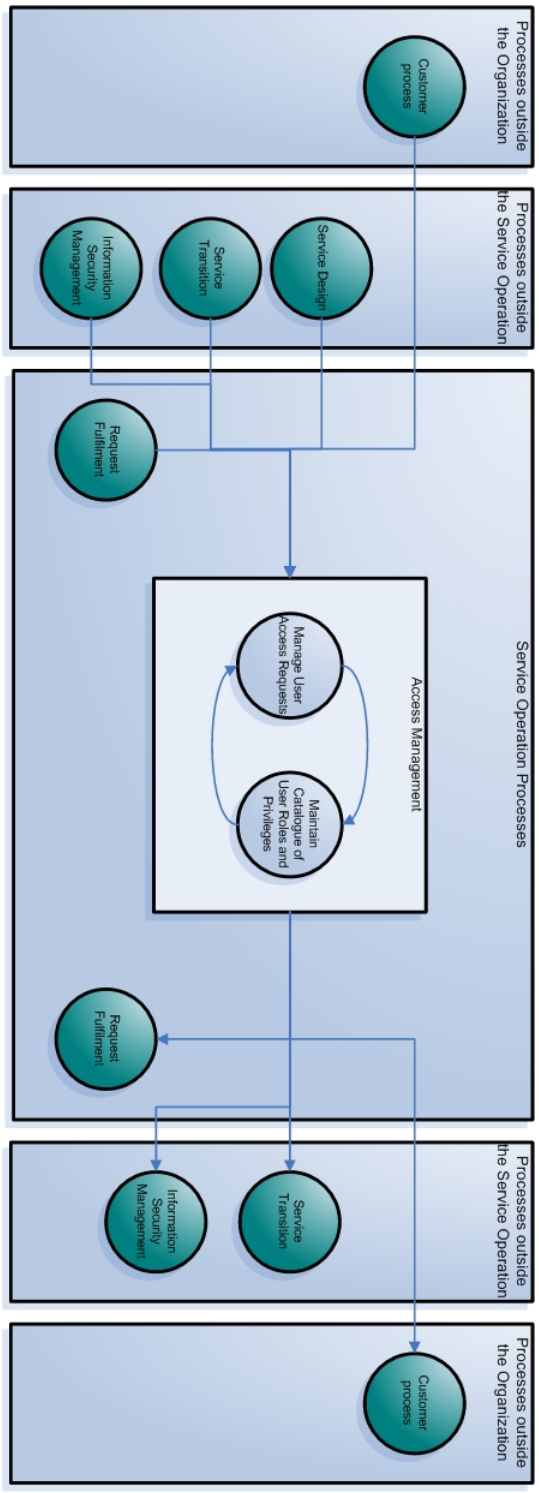
Taulukko 7: Vaatimusten prioriteetit.

Lyhenne	Nimi	Kuvaus
P	Pakollinen	Vaatimus on välttämätön toteutuksen kannalta.
T	Tärkeä	Vaatimus tuo huomattavaa lisäarvoa toteutukselle, mutta ei ole välttämätön.
A	Ajan salliessa	Vaatimus ei ole toiminnallisuuden kannalta oleellinen, mutta kannattava toteuttaa myöhemmässä vaiheessa.
E	Ei toteuteta	Vaatimus ei ole tärkeä, eikä sitä kannattava toteuttaa nykyisen tiedon valossa.
-	Ei priorisoitu	Vaatimukselle ei asetettu prioriteettia.

Vaatimukset sisältävät niiden nimen lisäksi lyhyen kuvauksen, mitä vaatimuksella tarkoitetaan, tai mitä sillä on tarkoitus saavuttaa. Vaatimukset ja niiden prioriteetit määriteltiin siten, että toteutusratkaisu toteutuessaan parantaisi oleellisesti pääsynhallintaa yrityksessä verrattaessa nykyiseen toteutukseen. Lisäksi toteutuksen tulee pystyä vastaamaan jollain tasolla myös tulevaisuuden tarpeisiin. Vaatimukset ja niiden prioriteetit on kuvattu taulukkoon 11 (liite B). Diplomityössä esitelty vaatimusmäärittely sisältää ylätason vaatimukset toteutusratkaisulle.

7.2 Pääsynhallinta palvelutoimintona

Pääsynhallinta määriteltiin olevan yksi palvelutoiminto IT palveluorganisaatiossa, jolle tulee luoda prosessikuvaus. Määrittelyssä pyrittiin täyttämään luvussa 2 esitellyt palveluhallinnan päätavoitteet, joita ovat: palvelun sovittaminen sekä yrityksen että asiakkaiden nykyisiin ja tuleviin tarpeisiin, parantaa tuotettujen palveluiden laatua ja niistä saatua kokemusta ja vähentää palvelun ylläpitämiseen vaadittavia kustannuksia. Kuten luvussa 2.1 mainitaan, jotta toimintatavalle voidaan myöhemmin hakea sertifiointia, tulee sen olla linjassa alan parhaiden käytäntöjen kanssa. Pääsynhallinnan prosessikuvaus suunniteltiin perustuen yrityksen yleiseen palvelutoimintaan ja ITIL v3 kuvaukseen [1, s. 68-71] pääsynhallinnasta. Diplomityössä esitelty pääsynhallintaprosessi on kuvattu ylätasolla kuvaan 13. Kuva tehtiin osana diplomityötä ja sen perustana käytettiin ITIL v3 kuvausta pääsynhallinnasta.



Kuva 13: Pääsynhallinnan ylätason prosessikuvaus

Kuten luvussa 2 mainitaan, pääsynhallinta voidaan lukea osaksi palveluntoimitusprosesseja. Pääsynhallinnan päätoimintoja ovat käyttöoikeuspyyntöjen hallinta ja jaettujen käyttöoikeustietojen ylläpito. Varsinaisten käyttöoikeuspyyntöjen hakemisen prosessi kuvataan kappaleessa *7.3 Käyttöoikeuspyyntöjen prosessikuvaus*.

Luvussa 2 esiteltyjen palvelutoiminnan päätavoitteiden mukaisesti palvelut tulee sovittaa oman liiketoiminnan ja asiakkaiden tarpeiden mukaisesti. Asiakaskohtaiset prosessit (*Customer Processes*), politiikat ja määräykset tulee ottaa huomioon toteuttaessa pääsynhallinnan toimintoja asiakkaalle.

Tietoturvan hallinta (*Information Security Management*) tarjoaa turvallisuus- ja tietosuojapolitiikan, jota pääsynhallinnan tulee noudattaa [1, s. 68]. Sillä on myös rooli luvattomien pääsyjen tunnistamisessa ja vertailemisessa niitä käyttöoikeuksiin, joita pääsynhallinnan kautta on toimitettu.

Palveluiden suunnitteluvaiheessa (*Service Design*) tulee määritellä rooli- ja käyttöoikeustiedot, jotta pääsynhallinta voidaan tehokkaasti toteuttaa palvelulle [2]. Lisäksi palveluiden muutosprosessit (*Service Transition*), kuten muutostenhallinta (*Change Management*) ja konfiguraation hallinta (*Configuration Management*) tarjoavat pääsynhallinnalle tietoa ympäristöjen muutoksista ja mahdollisuuden tiedustella ympäristöissä olemassa olevia käyttöoikeustietoja [1, s. 69].

Käyttöoikeuspyyntö voi lähteä liikkeelle palvelupyyntöjen käsittelyprosessin kautta (*Request Fulfillment*) *Service Deskistä* tai varsinaisesti käyttöoikeuspyynnöille tarkoitetusta työkalusta. Vastaavasti myös pyyntöjen toteutus voidaan siirtää toteutettavaksi palvelupyyntöjen käsittelyprosessille, tai se voidaan toteuttaa osana käyttöoikeuspyyntöjen hallintaa. Tieto jaetuista käyttöoikeuksista toimitetaan oikeuden pyytäjälle ja saajalle, sekä tarvittaessa kaikille asiaankuuluville prosesseille ja asiakkaille.

Pääsynhallintaan liittyy myös muutamia tukitoimintoja, jotka pääsynhallinnan palvelutoiminnassa tulee ottaa huomioon:

- Henkilöstömuutosten seuraaminen: kaikki työnkuvaa muuttavat toimenpiteet, kuten työtehtävien vaihto, ylennykset, irtisanoutumiset ja erottamiset käynnistävät toimintoja pääsynhallinnassa. Tieto muutoksista tulee yleisesti henkilöstöhallinnasta tai esimiehiltä.

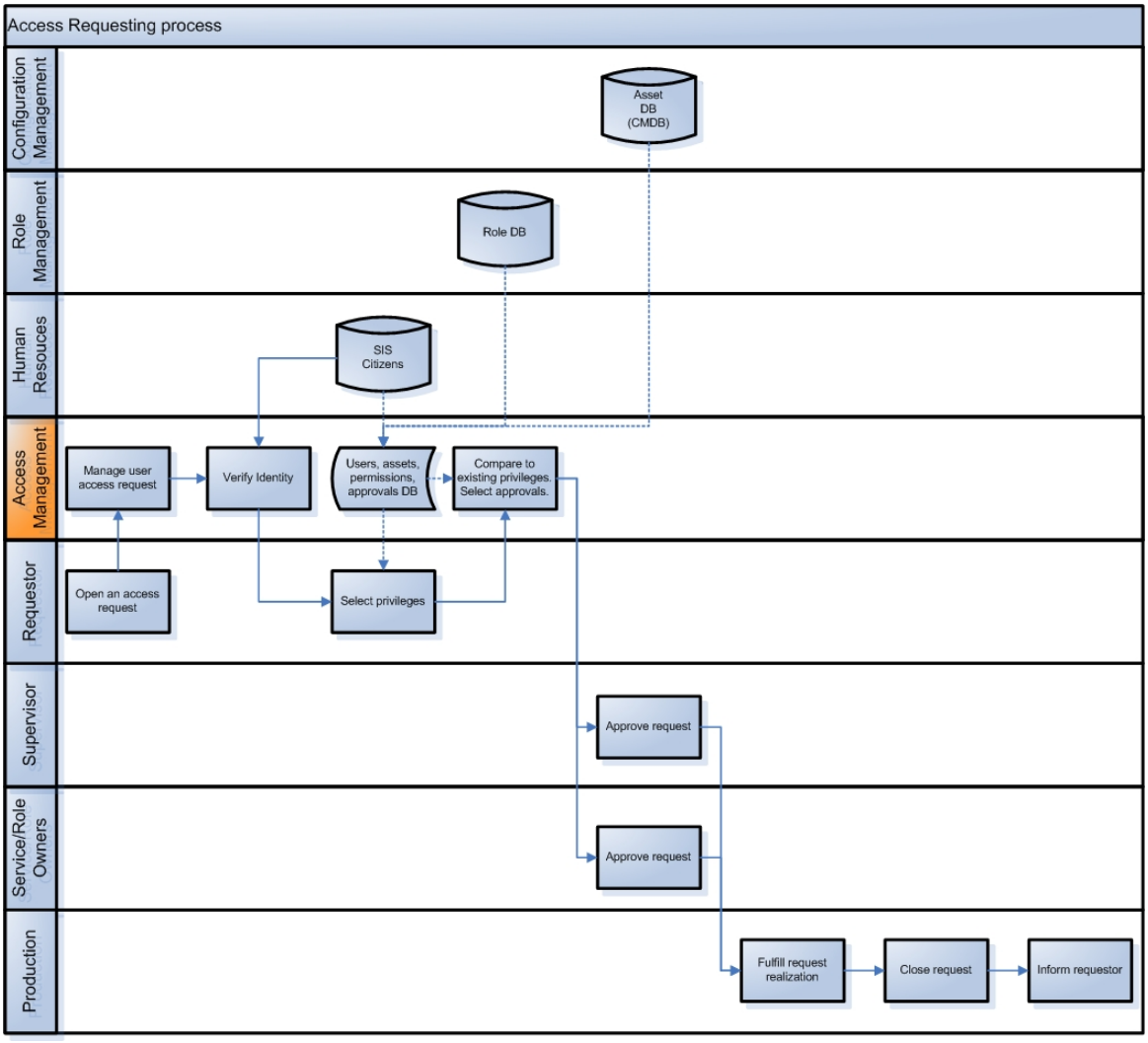
- Roolien hallinta: Erillinen palvelutoiminto, jota pääsynhallinta ohjaa. Roolien hallinta on vastuussa roolitietokantaan tietojen keräämisestä, määrittelemisestä ja ylläpitämisestä.

- Säännöllinen arviointi: Roolitietoja, käyttöoikeuskohteita ja niihin liitettyjä hyväksyjiä tulee arvioida säännöllisesti, jotta ne ovat sopivia niille määritellyille palveluille.

- Käyttöoikeustietojen auditointi: Käyttöoikeustietojen auditoinnilla ja pyritään varmistamaan, että oikeudet on jaettu oikeille henkilöille ja niitä käytetään oikein.
- Jatkuva palvelun kehitys: Palvelun toimintaa tulee jatkuvasti kehittää, jotta se vastaa yrityksen liiketoiminnallisiin tarpeisiin.

7.3 Käyttöoikeuspyyntöjen prosessikuvaus

Osana diplomityötä käyttöoikeuspyyntöjen käsittelyn vaiheista, vuorovaikutuksista ja vastuualueista tehtiin prosessikuva 14. Prosessikuvaus tarvitaan, jotta voidaan määritellä käyttöoikeuspyyntöihin liittyvät toiminnot ja niiden vastuualueet ottamatta kantaa itse toteutuksessa käytettävään työkaluun. Luotu käyttöoikeuspyyntöjen prosessikuvaus on suuntaa antava kuvaus, jota voidaan soveltaa tapauskohtaisesti erilaisiin käyttöoikeuspyyntöihin ja jota voidaan käyttää apuna määriteltäessä työkalua käyttöoikeuspyyntöjen hallintaan.



Kuva 14: Käyttöoikeuspyyntöjen prosessikuvaus

Käyttöoikeuspyyntö lähtee liikkeelle pyynnön luomisesta pyytäjän toimesta. Pyyntöjen vastaanottamisesta ja hallinnasta on vastuussa pääsynhallinta. Tämän lisäksi pääsynhallinta vastaa myös pyytäjän ja oikeudensaajan todentamisesta, valittavien käyttöoikeuskohteiden ja roolien toimittamisesta, olemassa olevien ja ristiriitaisten oikeuksien ja roolien tarkistamisesta sekä hyväksyjien valinnasta.

Toimintojen toteuttamiseen pääsynhallinta saa syötteitä muilta palvelutoiminnoilta: henkilötietoja henkilöstöhallinnalta, käyttöoikeus- ja roolitietoa roolienhallinnalta ja kohdejärjestelmätietoa konfiguraation hallinnalta. Oikeuden pyytäjä vastaa halutun käyttöoikeuskohteen ja oikeuden valinnasta pyyntöön.

Hyväksyjien määrittelyn jälkeen pyyntö ohjautuu vähintään kahdelle hyväksyjälle hyväksyttäväksi, joita yleensä ovat oikeuden saajan esimies ja käyttöoikeuskoh-

teen pääkäyttäjä tai palvelun palveluomistaja. Hyväksynnän jälkeen pyyntö siirtyy tuotannolle, joka vastaa oikeuden toteuttamisesta, pyynnön sulkemisesta ja toteutuksesta tiedottamisesta pyytäjälle ja oikeuden saajalle.

7.4 Identiteetinhallintamenetelmät

Koska yrityksessä on jo käytössä HR:n ylläpitämä henkilötietokanta, ei toteutusehdotuksen tarkoituksena ole korvata olemassa olevaa henkilötietokantaa. Lisäksi yrityksen verkkoidentiteettien ja verkkoresurssien hallintaa voidaan toteuttaa *Active Directoryn* avulla.

Identiteetin tunnistaminen pääsy- ja käyttöoikeuksia hakiessa tulisi perustua HR:n ylläpitämään henkilötietokantaan. Tällä tavalla pystytään todentamaan ja tunnistamaan henkilön asema yrityksessä yksiselitteisesti. Identiteetin tunnistaminen voitaisiin toteuttaa luvussa 4.1 mainitun jaetun paikallisen identiteetin mallin mukaisesti HR:n ylläpitämästä henkilötietokannasta.

Tunnistettuun identiteettiin tulisi pystyä lisäämään profiileja ja käyttövaltuuksia, jotta asianmukaista pääsynhallintaa voidaan toteuttaa. Toteutuksen tulee siis ylläpitää henkilörekisteriä käyttäjistä, joihin profiileja ja käyttövaltuuksia voidaan liittää. Osa käyttövaltuuksista toteutetaan *Active Directoryn* kautta verkkoidentiteettiin, jolloin toteutuksen pitää pystyä myös yhdistämään käyttövaltuuksia sisältävä identiteetti sitä vastaavaan verkkoidentiteettiin.

Lopputuloksena on yrityksen sisällä toimiva luvussa 4.3 esitellyn yhdistetyn identiteetin mallin mukainen toteutustapa, jossa osapuolina toimivat HR:n ylläpitämä henkilötietokanta, *Active Directory* ja pääsynhallinnan ylläpitämä henkilötietokanta. HR:n henkilötietokanta tarjoaa henkilön todentamiseen yrityksessä tarvittavat tiedot, ja sen pohjalta pääsynhallinta rakentaa oman henkilötietokantansa. Pääsynhallinnan henkilötietokannan identiteeteille voidaan liittää profiileja, roolitietoja ja tietoja yksittäisistä pääsyvaltuuksista. Pääsyvaltuudet voivat koskea mitä tahansa yrityksen ylläpitämää tietojärjestelmää ja resurssia. Pääsyvaltuudet, jotka koskevat *Active Directoryn* hallinnoimia resursseja, välitetään *Active Directoryn* verkkoidentiteeteille.

Toteutustavan etuina on yksinkertaisuuden säilyttäminen olemassa olevissa järjestelmissä, tuoden kuitenkin identiteeteille lisähallittavuutta profiilien ja käyttöoikeuksien muodossa. Lisäksi se mahdollistaa tehokkaan tavan kontrolloida käyttöoikeuksia yhdestä pisteestä. Toteutus on myös modulaarinen, mahdollistaen uusien identiteettirekisterien liittämisen siihen ilman, että se vaikuttaa olemassa olevien rekisterien toimintaan ja palveluihin.

7.5 Pääsynhallintamenetelmät

Jotta pääsynhallinta olisi osa luotettua tietojenkäsittelypohjaa (TCB), tulee sen toimia ylätason *Reference Monitorina*, kertoen identiteetteihin liitetyt pääsyvaltuudet, jota vasten voidaan kunkin identiteetin todelliset pääsyoikeudet tarkistaa. Lisäksi sen tulee tarjota rajapinta käyttöoikeuspyyntöjen luomista varten sisältäen identiteetin tunnistamisen ja varmistamisen.

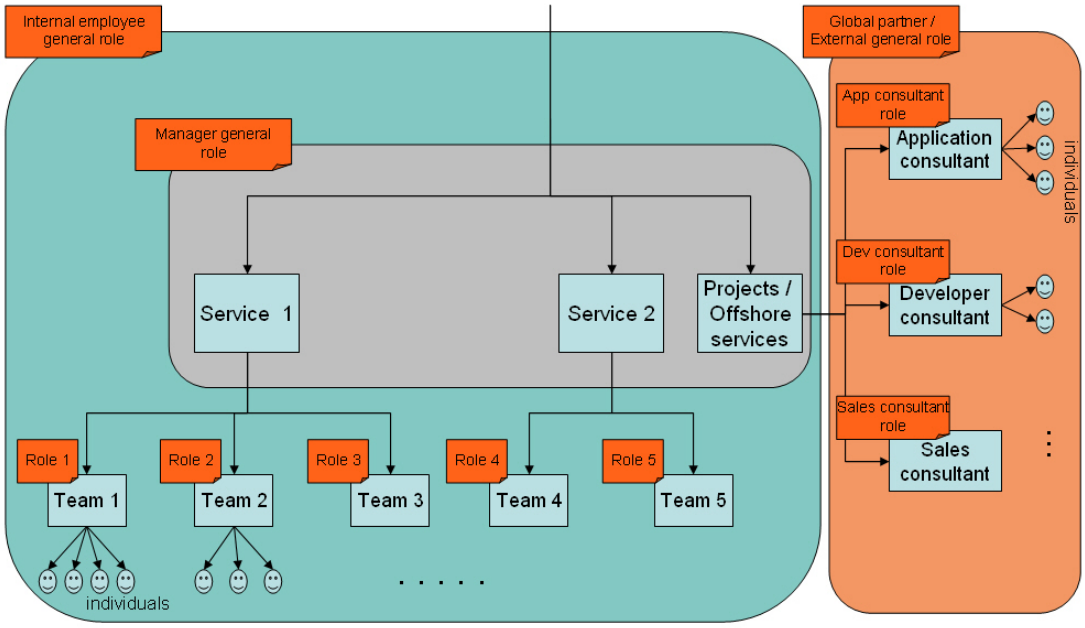
Toteutuksen tulisi perustua luvussa 5.2 esiteltyyn harkinnanvaraisen pääsynhallinnan malliin, sillä yrityksen lähes kaikki kohdejärjestelmät on määritelty resurssi-omistajuus mallin mukaisesti. Tämän lisäksi, tehostaakseen yleisten käyttöoikeuksien jakamista, pääsynhallinnan tulisi tukea luvussa 5.4 esitellyn roolipohjaisen pääsynhallinnan (RBAC) mukaista toimintatapaa. RBAC -menetelmän ei tarvitse toteutuksessa sulkea pois DAC -menetelmää, vaan luodut roolit voidaan myös ajatella resursseina ja näin määritellä niille omistaja resurssi-omistajuus mallin mukaisesti.

Koska kohdejärjestelmien käyttäjäkunta on suuri ja käyttäjien ja kohdejärjestelmien vaihtuvuus tiheää, tulee pääsynhallinnan perustua ehdottomasti suljettuun DAC menetelmään. Tällöin pääsy sallitaan vasta, kun pääsylle löytyy positiivinen valtuutus kohdejärjestelmään. DAC menetelmän haittapuolena pidetty käyttöoikeuksien harkitsematon leviäminen pyritään estämään noudattamalla yrityksen tietoturvapolitiikan mukaista neljän silmän periaatetta pääsyvaltuuksien hyväksynnöissä. Tällä tavoin pelkästään resurssien omistajat eivät voi myöntää valtuuksia resurssiin ja toteutus noudattaa luvussa 3.1.1 esiteltyä tehtävien eriyttämisen tietoturvapolitiikkaa.

7.6 Roolien määrittely

Roolien hallinnan määriteltiin olevan erillinen palvelutoiminto, kuuluen kuitenkin pääsynhallinnan alaisuuteen. Roolien hallinnan tehtävä on kerätä, määritellä ja ylläpitää roolitietokantaa ja niihin liittyviä oikeuksia. Roolien määrittelyssä pyrittiin ottamaan huomioon luvussa 3.1.2 esitelty tietoturvapolitiikka, pienimmän oikeuden periaate, säilyttäen kuitenkin käytännöllisyys ja oikeuksien riittävä kattavuus.

Osana diplomityötä tehtiin kuvaus roolien mallintamiselle yrityksessä. Lähtötason roolit määriteltiin kuvan 15 mukaisella tavalla, tavoitteena määritellä yleiset tasot rooleille ja pystyä vastaamaan suureen määrään yleisluonteisia käyttöoikeuspyyntöjä. Roolien määrittelyssä käytettiin luvussa 5.4.1 esiteltyjä *top-down* ja *bottom-up* menetelmiä. *Top-down* lähestymistavassa roolit määriteltiin toiminnallisten yksiköiden perusteella. *Bottom-up* menetelmällä kerättiin muodostetuille rooleille olemassa olevat ja tarpeelliset oikeudet. Olemassa olevien ja tarpeellisten oikeuksien kerääminen toteutettiin haastattelemalla yksiköiden esimiehiä ja täyttämällä tiedot keräämistä varten luotuun kaavakkeeseen (liite A).



Kuva 15: Roolien lähtötason määrittelemisessä käytetty malli

Pienimmiksi toiminnallisiksi yksiköiksi valittiin yrityksen organisaatioyksiköt. Kuvassa 15 näitä kuvataan tiimeillä *Team 1*:stä *Team 5*:een. Organisaatioyksiköiden käyttöön päädyttiin niiden sopivan koon, tunnistettavuuden ja määrän vuoksi. Lisäksi sääntöihin perustuva roolien liittäminen identiteetteihin onnistuu parhaiten organisaatioyksiköiden perusteella.

Palveluiden omistajien ja tiimien esimiesten katsottiin tarvitsevan hyvin samanlaisia oikeuksia keskenään, niinpä heille määriteltiin yleinen esimiestason rooli. Ulkoisille työntekijöille ja partnereille määriteltiin vain muutamia alustavia rooleja, joiden katsottiin kattavan suurimman osan heidän tarvitsemistaan käyttöoikeuksista.

Yrityksen sisäisille työntekijöille, ulkoisille työntekijöille ja partnereille määriteltiin yleiset peruskäyttöoikeudet sisältävät roolit. Peruskäyttöoikeudet sisältävät roolit eivät kata varsinaisiin työtehtäviin liittyviä oikeuksia, vaan yhteisiin työkaluihin, palveluihin ja tietueisiin liittyviä oikeuksia.

Roolien hallinta tukee muidenkin kuin organisaatioyksikköperustaisten roolien luomista. Periaatteessa mistä työnkuvasta tahansa voidaan luoda rooli, jos sille määritellään yhdessä tietoturvahallinnon kanssa vastuuhenkilö, joka vastaa roolin sisällöstä ja toimii hyväksyjänä roolille. Esitellyt lähtötason roolit pyrkivät vastaamaan suureen määrään yleisluontoisia käyttöoikeuspyyntöjä. Lisäksi jokaiselle käyttäjälle voidaan hakea mitä tahansa luotua roolia tai yksittäistä käyttöoikeutta. Oikeuden

hyväksymisestä vastaavat hyväksyjät.

7.7 Työkalun määrittely

Työkaluksi toteutukselle yritys oli ennalta valinnut DirX tuoteperheen. Työkalun valintaan on vaikuttanut muun muassa se, että työkalu on yrityksen omistama ja sen käytöstä on paikallista kokemusta yhteiskäyttötunnusten tietojen säilyttämisessä. Lisäksi muokattavuuden sekä modulaarisen rakenteen vuoksi toiminnallisuus ja rajapinnat voidaan määritellä paikallisiin tarpeisiin sopivaksi.

Työkalun käyttöönottoa varten tehtiin toiminnallinen määrittely, jolla kuvattiin toteutuksen kannalta tarvittavat toiminnallisuudet ja rajapinnat, joita työkaluun tarvitsee toteuttaa. Lisäksi määriteltiin työkaluun toteutettavat provisointitavat. Varsinainen tekninen toteutus ja työkalun käyttöönotto jätettiin tutkimustyön ulkopuolelle.

7.7.1 DirX

DirX on Atoksen omistama tuoteperhe, jolla voidaan tarjota keskitetty identiteetin- ja pääsynhallinta yrityksille [34]. Tuoteperheeseen kuuluu neljä keskeistä tuotetta [34]:

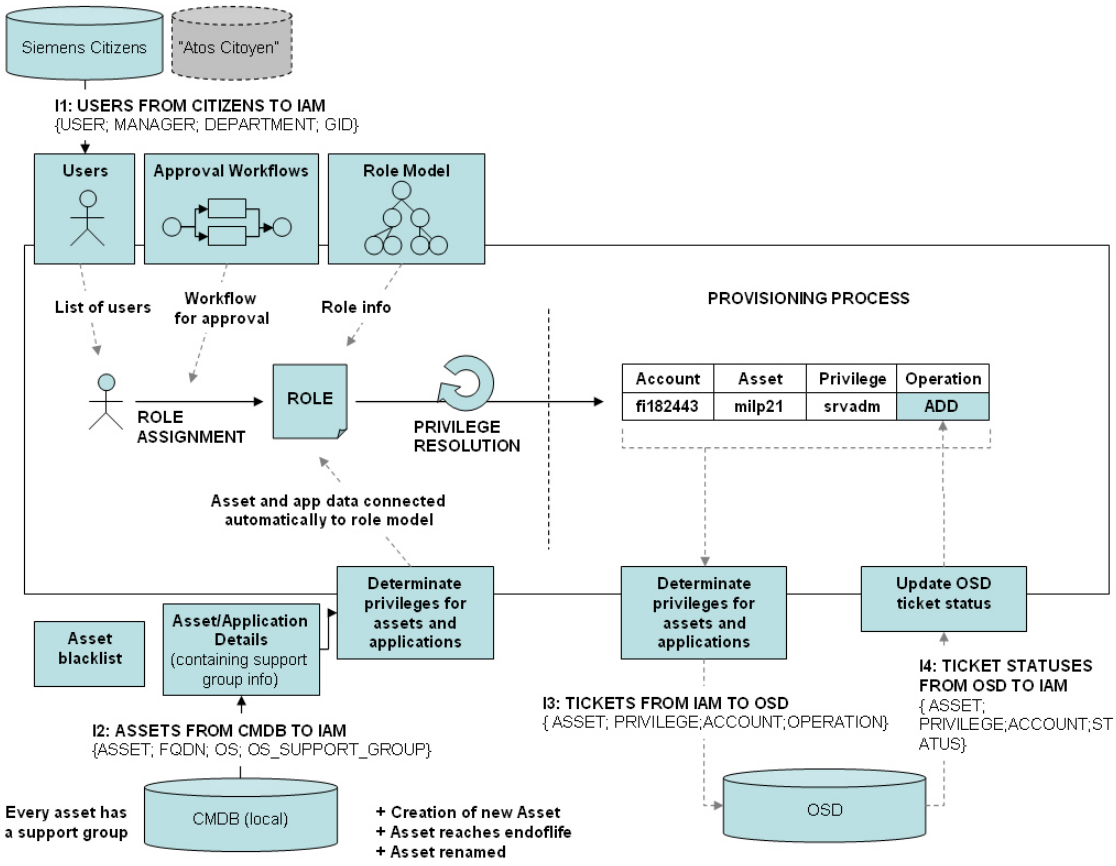
- DirX Identity, tarjoaa automatisoidun käyttäjien ja käyttöoikeuksien hallintaan ja jakamiseen tarkoitetun järjestelmän.
- DirX Audit, tarjoaa keskitetyn alustan käyttöoikeustietojen keräämiselle, varastoinnille ja analysoinnille.
- DirX Directory, mahdollistaa turvallisen varastoinnin digitaalisille identiteeteille ja on suunniteltu käsittelemään hyvinkin suuri määrä käyttäjiä.
- DirX Access, mahdollistaa luvun 4.3 mukaisen yhdistetyn identiteetin ja kertakirjautumismenetelmän luomisen järjestelmiin tarjoten samalla turvamekanismeja luvattomien pääsyjen estämiseksi.

Tässä diplomityössä ei erikseen eritellä millä tuoteperheen tuotteella mikäkin toteutuksen osa on tarkoitus toteuttaa, vaan puhutaan yleisesti DirX:stä tai IAM-työkalusta.

7.7.2 IAM-työkalun toiminnallisuuden määrittely

Työkalun toiminnallinen määritelmä tehtiin perustuen luvussa 7.1 esiteltyyn pääsynhallinnan vaatimusmäärittelyyn ja työkalun käytöstä yhteiskäyttötunnusten tietojen säilyttämisessä saatuun kokemukseen. Toiminnallisuuden määrittely jaettiin

osiin: rajapinnat ja tietolähteet sekä toiminnot. Toiminnallisuudesta tehtiin diplomityön puitteissa havainnekuva, kuva 16, jossa rajapinnat ja tietolähteet on merkattu I1:stä I4:ään ja toiminnot sinisiin laatikoihin ja nuoliin.



Kuva 16: DirX toiminnallisuuden kuvaus

Rajapinnat ja tietolähteet määrittelevät mitä tietoa työkalulle tarvitsee antaa, miksi ja mistä tieto saadaan. Rajapintamääritys ei kuitenkaan ota kantaa miten varsinainen tiedonsiirto toteutetaan.

I1: Käyttäjätieto yrityksen HR-järjestelmästä. Tiedon perusteella työkaluun synkronoidaan paikallinen käyttäjärekisteri, joka vastaa HR:n ylläpitämää tietoa. Tiedot luetaan päivittäin ja käyttäjien lisäykset ja poistot tehdään automaattisesti perustuen luettuun tietoon. Tiedon tulee sisältää riittävästi tuntomerkkejä käyttäjistä, kuten yksilöllinen henkilönumero, organisaatioyksikkö ja esimies, jotta heidät voidaan tunnistaa ja jotta heille voidaan määritellä roolit ja esimieshyväksyjät.

I2: Kohdejärjestelmätieto yrityksen CMDB:stä (konfiguraatiotietokanta). Tiedon perusteella työkaluun kerätään kohdejärjestelmät ja haettavat käyttöoikeudet. Tarpeettomat kohdejärjestelmät karsitaan pois vertaamalla haettua tietoa määriteltyyn mustaan listaan. Kohdejärjestelmien tuntomerkkien tietojen perusteella kohdejärjestelmät voidaan määritellä kuuluvaksi osaksi tiettyä roolia ja määritellä siihen jaettavien oikeuksien provisiointikanava.

I3: Oikeuksien toteutustieto IAM-työkalusta oikeaan provisointikanavaan. Provisointi voi olla toteutettu esimerkiksi tiketöintijärjestelmän kautta, jolloin haettavasta oikeudesta avataan palvelupyyntö oikealle toteutustiimille.

I4: Toteutuksen tilatiedot provisointikanavasta IAM-työkaluun. Jos oikeus provisioidaan muuten kuin suoraan kohdejärjestelmään, esimerkiksi sähköpostina tai tiketöintityökalun kautta, tulee toteutuksen etedistymisestä saada tilatiedot takaisin IAM-työkaluun. Toteutuksen onnistumisesta tarvitaan kuittaus, jotta oikeus voidaan merkitä toimitetuksi käyttäjälle.

Toiminnot määrittelevät mitä työkalun tulee pystyä tekemään siihen syötetyllä ja määritellyllä tiedolla. Määritelmäkuvaukset eivät ota kantaa siihen, miten toiminnallisuus varsinaisesti työkaluun toteutetaan.

Kohdejärjestelmätiedon tulkitseminen käyttöoikeuskohteiksi. Kohdejärjestelmätieto puretaan auki ja perustuen järjestelmien tuntomerkkeihin jaetaan rooleihin ja käyttöoikeuskohdelistaukseen haettaviksi kohteiksi. Tuntomerkkien perusteella asetetaan myös provisiointikanava kohteille.

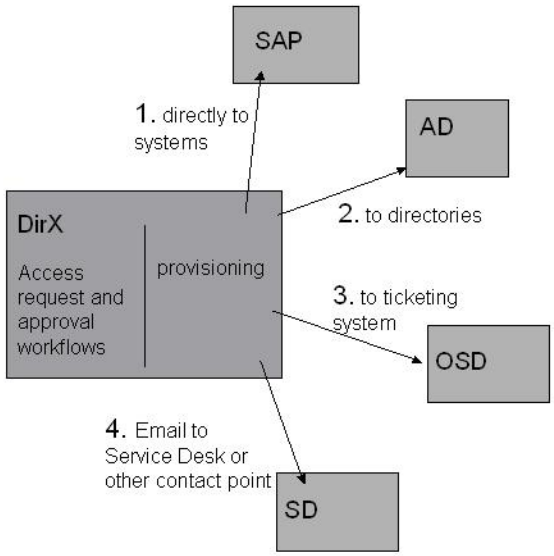
Roolien mallintaminen käyttäjille. Käyttäjille osoitetaan roolit automaattisesti perustuen käyttäjien tuntomerkkitietoihin. Roolitieto lasketaan auki oikeuksiksi ja käyttäjän olemassa olevia oikeuksia verrataan roolitietojen sisältämiin oikeuksiin. Haettavista oikeuksista luodaan esihyväksytyt oikeuspyynnöt, jossa esihyväksyntä perustuu oikeuden saamiseen roolin kautta. Vastaavasti käyttäjän itse hakiessa roolia, puuttuvista oikeuksista lähetetään hyväksyntäpyyntö esimiehelle ja kohdejärjestelmien palveluomistajille.

Oikeuksien aukilaskenta ja provisiointi. Haettavat käyttöoikeuskohteet jaotellaan provisiointikanavan ja toteutustiimin perusteella ryhmiin ja tämän jälkeen

haettavat oikeudet tulkataan kullekin provisiointikanavalle soveltuvaan muotoon ja siirretään provisioitavaksi. Provisiointikanavista saaduilla tilatietopäivityksillä pidetään kirjaa oikeuksien toteutuksen etenemisestä.

7.7.3 Oikeuksien provisiointi

Käyttöoikeuksien provisiointi suunniteltiin voivan toteuttaa kohdejärjestelmästä riippuen neljällä eri tavalla: 1) suora liitäntä kohdejärjestelmiin, 2) liitäntä *Active Directory* -hakemistopalveluun, 3) tiketöintijärjestelmän kautta tai 4) sähköpostiviestin avulla. Prosiviointisuunnitelmasta tehtiin diplomityön puitteissa havainnekuva 17. Työkalu mahdollistaa kaikkien näiden provisiointimenetelmien toteuttamisen. Usean provisiointikanavan käyttäminen lisää vikasietoisuutta, sillä oikeuksien toteuttaminen ei ole riippuvainen yhdestä provisiointikanavasta. Lisäksi se mahdollistaa optimaalisimman provisointikanavan käyttämisen kohdejärjestelmäkohtaisesti, jolloin oikeuksien toteuttaminen on mahdollisimman tehokasta. Toisaalta, usean provisiointikanavan toteuttamisessa ja käyttämisestä on myös haasteita, sillä usean provisointikanavan toteutus työkaluun vaatii paljon työtä toteutuksellisesti ja ylläpidollisesti.



Kuva 17: Oikeuksien provisiointikanavat

1. **Suora liitäntä kohdejärjestelmiin.** Kaikkein tehokkain tapa oikeuksien saamisen kannalta on provisioida oikeuksia suoraan kohdejärjestelmään. Tällöin IAM-työkalu määrittää välittömästi oikeuden hyväksynnän jälkeen kohdejärjestelmään, kenellä on sinne tietyllä oikeustasolla pääsy. Myös oikeuksiin tapahtuvat muutokset, kuten tunnuksien lukitsemiset ja poistot, tapahtuvat välittömästi ja näin parantavat tietoturvaa. Suora liitäntä kohdejärjestelmiin mahdollistaa myös hyvin ajantasaisen ja tarkan tiedon siitä, kenellä on oikeuksia mihinkin järjestelmään. Ongelmana suorassa liitännässä on liitäntätyön määrä. Lähes jokainen kohdejärjestelmä joudutaan liittämään erikseen ja liitäntöjen rajapintamääritykset voivat vaihdella kohdejärjestelmien välillä. Tiheästi muuttuvissa ympäristöissä vaadittu työmäärä suorien liitäntöjen tekemiseen ei ole kannattavaa verrattaessa saatuun hyötyyn, vaan liitännät tulisi rajata ympäristöihin, joissa tapahtuu vähän muutoksia, mutta joissa on suuri käyttöaste.

2. **Active Directory.** Liitäntä hakemistopalveluun, kuten *Microsoft Active Directoryyn*, tuo hyvin samanlaiset hyödyt kuin suora liitäntä kohdejärjestelmiin. IAM-työkalu määrittää pääsyoikeudet ja niiden tasot *Active Directoryn* käyttäjätietokantaan ja hakemistopalveluun mahdollistaen tehokkaan pääsyoikeuksien jakamisen siihen kuuluville käyttäjille. Oikeuksien toteutuminen tapahtuu välittömästi, samoin niihin kohdistuvat muutokset. Liitäntä hakemistopalveluun mahdollistaa hyvin ajantasaisen ja tarkan tiedon toteutetuista oikeuksista eri järjestelmiin. Liitännät tarvitsee tehdä vain käytössä oleviin *Active Directory* hakemistopalveluihin, jolloin liitäntöjen määrittämiseen ja tekemiseen vaadittu työmäärä ei kasva suureksi. Ongelmana *Active Directory* liitäntöjen tekemisessä on, että se vaatii vahvan luottamussuhteen IAM-työkalun ja siihen liitettyjen hakemistopalveluiden välille. Liitäntä voi olla vaikea saada hyväksyttyä *Active Directoryihin*, joilla hallinnoidaan asiakasympäristöjä. Lisäksi suuri määrä kohdejärjestelmiä ei ole liitetty *Active Directoryyn*, kuten Unix-järjestelmät ja SAP-ympäristöt. Tällaisiin järjestelmiin oikeuksien provisiointi tarvitsee toteuttaa muulla tavalla.

3. **Tiketöintijärjestelmä** Oikeuksien provisiointi tiketöintijärjestelmään mahdollistaa pääsyoikeuden toteuttamisen lähes mihin tahansa kohdejärjestelmään, mikä tekee siitä vikasietoisen provisiointitavan. Perustuen kohdejärjestelmän tukiryhmään, IAM-työkalu luo pyydetystä oikeudesta palvelupyynnön tiketöintijärjestelmään oikealle toteutustiimille varsinaiseen toteutukseen. Liitäntä tiketöintijärjestelmään ei tarjoa välitöntä oikeuden toteutusta, mutta säästää kuitenkin manuaalista työtä palvelupyynnön luomisessa. Lisäksi pyyntö voi kohdistua järjestelmään, joka ei olisi muuten mahdollista liittää IAM-työkaluun. Ongelmana tiketöintijärjestelmän käytössä on työmäärä, joka tarvitaan kohdejärjestelmien tukiryhmätietojen tarkistamiseen ja oikeiden toteutustiimien määrittämiseen niille. Eri kohdejärjestelmiä koskevat pääsyoikeudet tulee pystyä ohjaamaan oikeille toteutustiimeille. Lisäksi oikeuden varsinainen toteutus vaatii aina manuaalista työtä toteutustiimiltä. Provisiointi tiketöintijärjestelmään ei myöskään takaa ajantasaista ja täydellistä varmuutta käyt-

täjien pääsyoikeustietojen todellisesta tilasta.

4. **Sähköposti** IAM-työkalun konfiguraation määrittämisen ja sen ylläpitämisen kannalta helpoin tapa provisioida oikeuksia on lähettää niiden tiedot sähköpostilla *Service Deskiin*. IAM-työkalu luo haetuista oikeuksista viestin, joka sisältää tiedon siitä, millaiset oikeudet tarvitaan, mihin ja kenelle. Viesti lähetetään *Service Deskiin*, joka tulkitsee viestin ja luo siitä palvelupyynnön tiketöintijärjestelmään. Sähköpostin käyttö on hyvin vikasietoinen provisiointitapa sen yksinkertaisuuden vuoksi ja sillä voidaan hakea oikeutta lähes mihin tahansa kohdejärjestelmään. Ongelmana sähköpostiliitännässä on, ettei se tarjoa mitään automaatiota ja oikeuksien toteutuksen kannalta parannusta verrattaessa yrityksen olemassa oleviin käyttöoikeuspyyntöjen hallintaratkaisuihin. Manuaalinen työmäärä säilyisi edelleen *Service Deskissä* ja toteutustiimissä. Oikeuksien provisiointi sähköpostiliitännän kautta ei myöskään takaa ajantasaista ja täydellistä varmuutta käyttäjien pääsyoikeustietojen todellisesta tilasta.

8 Arviointi, yhteenveto ja jatkotutkimus

Luvussa 7 esitelty toteutusehdotus arvioitiin vertailemalla sitä luvussa 6 käsiteltyyn tapaustutkimukseen ja sen tuloksiin ja luvussa 1.3 esiteltyjä arviointikriteerejä vasten. Varsinaisesta teknisestä toteutuksesta ei ole tuloksia, sillä työkalun käyttöönotto ei kuulunut tämän diplomityön rajaukseen.

8.1 Arviointi

Tapaustutkimuksesta saatujen tulosten perusteella yrityksen nykyinen pääsynhallinnan toteutus on puutteellinen monelta osin. Toteutusehdotuksessa esitelty ratkaisu tarjoaisi keskitetyn ratkaisun nykyisen kahden, osittain päällekkäin toimivan, työkalun tilalle. Käyttöoikeuksien hakemiselle voitaisiin luoda yksiselitteinen ohjeistus ja toimintatapa. Lisäksi toteutusehdotus mahdollistaisi ajantasaisen identiteettien ylläpitämisen sekä profiilien, roolien ja pääsyvaltuuksien liittämisen niihin. Toisin kuin ARAP:ssa ja CIR:ssä, toteutusehdotuksessa esitelty työkalu tukee roolipohjaista pääsynhallintaa ja automatisoitua, sääntöihin perustuvaa käyttöoikeuksien ja roolien jakamista.

Toteutusehdotuksen toteutuskelpoisuutta arvioitiin tarkastelemalla toteuttamiseen vaadittavia laite- ja ohjelmistoinvestointien sekä henkilöresurssien määrää ja toteutukseen kuluvaa aikaa. Toteutukseen valittu työkalu on yrityksen omistama ja yritys tuottaa itse palvelimien ja palveluiden ylläpitotoimintoja, mistä johtuen toteuttamiseen vaaditut ohjelmisto- ja laiteinvestoinnit ovat vähäiset, eivätkä ole esteenä toteutukselle. Henkilöresurssien määrää ja toteutukseen kuluvaa aikaa tarkasteltiin työkalun käyttöönottoa varten laaditun projektisuunnitelman pohjalta. Projektisuunnitelman mukaan toteutus vaatisi noin 400 henkilötyöpäivää ja ajallisesti olisi mahdollista toteuttaa reilussa puolessa vuodessa. Arvio tarvittavien resurssien määrästä ja aikataulusuunnitelmasta on kohtuullinen, vaadittu osaamistaso löytyy suurelta osin yrityksen sisältä, ja heidän saaminen projektin käyttöön on mahdollista. Toteutusehdotus on henkilö- ja aikaresurssien sekä investointien osalta toteutuskelpoinen yrityksen kokoon ja liikevaihtoon nähden.

Toteutusehdotuksen taloudellista kannattavuutta arvioitiin tekemällä laskelma siitä, miten paljon säästöjä toteutuksella voidaan saavuttaa verrattaessa nykyiseen toimintatapaan. Kannattavuuslaskelma perustuu arvioihin, mitä toteutusehdotuksella oletetaan saavutettavan lyhyellä aikavälillä. Tavoitteena on saavuttaa projektiin käytetty työmäärä vuoden sisällä toteutuksesta. Arviota varten tutkimuksessa tehtiin taulukon 8 mukaiset lähtöoletukset toteutukselle.

Taulukko 8: Lähtöoletukset, jotka toteutusehdotuksen oletetaan täyttävän

Nro.	Olettamus
1	80% Sharepoint pyynnöistä voidaan määritellä rooleihin, jolloin oikeuksien hakemiseen ja hyväksymiseen ei kulu aikaa.
2	30% Muista pyynnöistä voidaan määritellä rooleihin, jolloin oikeuksien hakemiseen ja hyväksymiseen ei kulu aikaa.
3	80% Sharepoint pyynnöistä provisioidaan AD:iin.
4	20% Sharepoint pyynnöistä provisioidaan OSD:iin.
5	5% Muista pyynnöistä provisioidaan joko AD:iin tai suoraan kohdejärjestelmiin.
6	45% Muista pyynnöistä provisioidaan OSD:iin.
7	50% Muista pyynnöistä provisioidaan sähköpostiin.
8	Provisiointi AD:iin tai suoraan kohdejärjjestelmiin ei kuluta kenenkään työaikaa.
9	Provisiointi sähköpostiin kuluttaa Service Deskin ja tuotantotiimin työaikaa samoin kuin CIR:n tapauksessa.
10	Provisiointi sähköpostiin kuluttaa oikeuden saajan odotusaikaa samoin, kuin CIR:n hyväksymisestä sulkeutumiseen kulunut aika.
11	Provisiointi OSD kuluttaa tuotantotiimin työaikaa samoin, kuin ARAP:n hyväksymisestä sulkeutumiseen kulunut aika.
12	Provisiointi OSD kuluttaa oikeuden saajan odotusaikaa samoin, kuin ARAP:n hyväksymisestä sulkeutumiseen kulunut aika.
13	Oikeuden saajan odotusaika muutetaan menetetyksi työajaksi seuraavalla tavalla: odotusajan tunnit muutetaan viikoksi (tunnit/24/7), viikot muutetaan työtunneiksi (viikot*37,5), 10% työtunneista katsotaan menetetyksi työajaksi (tunnit*10%).
14	Neljän silmän periaatteen mukaisesti hyväksynnissä käytetään vähintään kahta hyväksyjää. Hyväksyntään käytetty työaika kerrotaan kahdella.
15	Käyttöoikeuspyyntöjen hakemiseen ja hyväksymiseen kuluva aika on sama, kuin ARAP:ssa ja CIR:ssa.
16	Pyynnöt joita ei jaeta automaattisesti vaan katsotaan haettavan manuaalisesti manuaalisesti, kuluttavat oikeuden saajan odotusaikaa samalla tavalla, kuin ARAP:n avaamisesta hyväksymiseen kulunut aika.

Tapaustutkimuksessa kerättyjen tulosten perusteella laskettiin käyttöoikeuspyyntöihin käytetty työaika kuukautta kohden ARAP:n ja CIR:n osalta. Käytettyihin työaikoihin laskettiin mukaan oikeuden saajan odotusajasta laskettu menetetty työaika olettamuksen nro. 13 mukaisesti. Taulukkoon 9 on laskettu ARAP:n ja CIR:n osalta käyttöoikeuspyyntöihin käytetty työaika kuukautta kohden. Yhteenlaskettuna käyttöoikeuspyyntöihin kuluu arviolta 1520 h/kk.

Taulukko 9: Käyttöoikeuspyyntöihin käytetty aika ARAP:ssa ja CIR:ssä kuukautta kohden

	ARAP	**CIR**
Pyyntöjä keskimäärin kuukaudessa		
Sharepoint		76
Muut	109	73
Käytetty työaika pyyntöä kohden		
Pyynnön avaamiseen	15 min	15 min
Pyynnön hyväksymiseen	5 min	5 min
Koordinaattorin työ	15 min	
Service Desk pyynnön vastaanotto ja tiketin luonti		5 min
Tuotantotiimi toteutus	15 min	15 min
Vastaanottajan menettämä työaika (olettamus 13)		
Avaamisesta hyväksymiseen	3,1 h	2,9 h
Hyväksymisestä sulkemiseen	1,1 h	2,9 h
Käytetty työaika yhteensä:		
		91200 min
		1520 h

Toteutusehdotuksen mukaisen toimintatavan arvioitu käyttöoikeuspyyntöihin käytetty työaika on laskettu taulukkoon 10. Lasketussa arviossa käytetään taulukon 8 mukaisia olettamuksia toteutuksesta.

Taulukko 10: Arvio toteutusehdotuksessa käyttöoikeuspyyntöihin kuluvasta ajasta

Arvio uudella työkalulla kuluvasta ajasta	**DirX**
Käytetty työaika avaamiseen ja hyväksymiseen sekä vastaanottajan menettämä työaika	
80% Sharepoint pyynnöt (RBAC)	0 min
20% Sharepoint pyynnöt (manuaaliset pyynnöt)	3311 min
30% Muut pyynnöt (RBAC)	0 min
70% Muut pyynnöt (manuaaliset pyynnöt)	27755 min
Hyväksymisen jälkeiset työvaiheet	
80% Sharepoint pyynnöt (AD provisiointi)	0 min
20% Sharepoint pyynnöt (OSD provisiointi)	1205 min
5% Muut pyynnöt (AD/suora provisiointi)	0 min
45% Muut pyynnöt (OSD provisiointi)	6493,5 min
50% Muut pyynnöt (Sähköpostiprovisiointi)	17700 min
Yhteensä:	
	56400 min
	940 h

Taulukoista 9 ja 10 voidaan laskea toteutusehdotuksen tuoma hyöty. Toteutusehdotuksen arvioidaan tuovan työaikasäästöä kuukaudessa 1520 h/kk - 940 h/kk = 580 h/kk. Vertaamalla kuukausittaista hyötyä projektisuunnitelman arvioituun työmääräarvioon, joka oli 400 henkilötyöpäivää, eli 3000 työtuntia, voidaan karkeasti arvioida toteutuksen takaisinmaksuajan työmäärän osalta olevan 3000 h / 580 h/kk = 5 kk.

Toteutusehdotuksen tuomaa työaikasäästöä tarkastellessa toteutusehdotus täyttää taloudellisen kannattavuuden kriteerin. Lisäksi toteutusehdotus tuo laadullista lisäarvoa yrityksen pääsynhallintaan muun muassa tarjoamalla tarkemman ja ajantasaisemman olemassa olevien käyttöoikeuksien tarkastelun, ja lisäämällä automaatiota ja tietoturvaa RBAC -mallin käyttöönoton myötä.

Toteutusehdotuksen ylläpidettävyyden ja käytettävyyden arvio perustuu aikaisempaan kokemukseen DirX työkalusta. Työkalun ja siihen konfiguroidun sisällön ylläpidettävyys ja päivitettävyys vaatii ylläpitäjältä tietyn tason osaamista työkalusta. Toiminnot ovat kuitenkin hyvin johdonmukaisia ja selkeitä, ja työkalu ei tarvitse päivittäisiä ylläpitotoimintoja. Riittää, että aika ajoin toiminnallisuus tarkistetaan ja tarvittaessa sisältöön tai toiminnallisuuteen pyydetyt muutokset toteutetaan. Työkalusta on olemassa paljon dokumentaatiota ja osaamista yrityksen sisällä, jolloin koulutusta on mahdollista tarjota uusille ylläpitäjille hyvinkin nopeasti. Loppukäyttäjän näkökulmasta käytettävyyttä voidaan muokata hyvinkin paljon. Loppukäyttäjät käyttävät työkalua web-portaalin kautta, joka on täysin muokattavissa haluttujen toiminnallisuuksien ja ulkoasun mukaan.

Turvallisuutta arvioitiin tarkastelemalla toteutusehdotuksen turvallisuuteen liittyviä ominaisuuksia. Toteutusehdotuksen avulla pystytään toteuttamaan dynaaminen tehtävien eriyttäminen oikeuksien hakemisessa ja noudattamaan neljän silmän periaatetta oikeuksien hyväksymisessä. RBAC -mallin käyttöönotto lisää osaltaan tietoturvaa mahdollistaen ennalta määritellyt roolikuvaukset työntekijöille ja oikeuksien jakamisen niihin perustuen. RBAC -mallin avulla saavutetaan luottamuksellisuus, eli tietoa luovutetaan vain heille, joilla on oikeus tietoon. Verrattaessa tapaustutkimuksessa kuvattuihin ARAP:iin ja CIR:iin, toteutusehdotus tarjoaa useita tietoturvaa lisääviä ominaisuuksia, kuten ajantasaisen tiedon olemassa olevista käyttöoikeuksista, yhtenevän käyttäjätietokannan HR:n kanssa, mahdollisuuden hakea kohdejärjestelmätiedot suoraan CMDB:stä ja nopeamman käyttöoikeuksien provisioinnin kohdejärjestelmiin. Nämä ominaisuudet takaavat tietoturvatavoitteiden mukaisen pääsynhallintatiedon saatavuuden, eheyden ja aitouden ja kiistämättömyyden.

Skaalautuvuutta arvioitiin tarkastelemalla miten hyvin toteutusehdotus pystyy ottamaan huomioon käyttäjäkunnan ja järjestelmien määrän ja niissä tapahtuvat muutokset. Toteutusehdotus vastaa käyttäjäkunnan muutoksiin rakentamalla paikallisen käyttäjärekisterin tietokantaan yrityksen HR-järjestelmän tietojen pohjalta. Tiedot luetaan päivittäin ja käyttäjien lisäykset ja poistot tehdään automaattisesti perustuen luettuun tietoon. Verrattaessa tapaustutkimuksessa kuvattuihin ARAP:iin ja CIR:iin, toteutusehdoksen käyttäjäkunnan hallinta on hyvin samankaltainen kuin CIR:ssä. Vastaavasti kuin käyttäjätietojen ylläpitäminen, kohdejärjestelmätiedot voidaan lukea yrityksen CMDB:ia ja rakentaa sen pohjalta työkaluun oma kohdejärjestelmätietokanta. Tiedot voidaan määritellä luettavaksi päivittäin ja lisäysten ja poistojen toteutus automatisoida. Verrattaessa tapaustutkimuksessa kuvattuihin ARAP:iin ja CIR:iin, kohdejärjestelmien lukeminen CMDB:sta on huomattava parannus mahdollistamalla ajantasaisen kohdejärjestelmätiedon tuomisen pääsynhallinnan piiriin. Toteutusehdotuksessa esitelty työkalu DirX mahdollistaa suurienkin tietokantojen hallinnoimisen.

Toteutusehdotuksessa esitelty pääsynhallinta palvelutoimintona arvioitiin olevan linjassa alan parhaiden käytäntöjen (ITIL v3, COBIT Guidance to Achieve Control Objectives for Successful IT Governance) kanssa. Toteutusehdotuksen mukaiselle pääsynhallinnalle voidaan yrityksessä lähteä hakemaan standardien mukaista sertifiointia.

8.2 Yhteenveto

Yleisesti pääsynhallinnan toteuttamiseen yrityksissä ei ole yhtä oikeaa toteutustapaa. Useissa tapauksissa toteutuksen suhteen tarvitsee tehdä kompromisseja tehokkuuden, turvallisuuden, käytettävyyden, muokattavuuden ja kustannusten välillä. IT-ulkoistuspalveluntarjoajan näkökulmasta pääsynhallinnan tulee kyetä vastaa-

maan suureen määrään käyttäjiä ja erilaisia ympäristöjä säilyttämällä yrityksen tietoturvapolitiikan määrittelemä tavoiteltu tietoturvataso. Jos pääsynhallinnalle palveluna halutaan hakea sertifiointia, tulee se kuvata palvelutoiminnoksi, joka on linjassa alan parhaiden käytäntöjen kanssa.

Tapaustutkimuksessa saaduista tuloksista voidaan todeta, että pääsynhallinta vaatii aina jatkuvaa kehittämistä ja valvontaa, varsinkin, jos sen on tarkoitus pystyä vastaamaan yritysten tarpeisiin ympäristöjen ja käyttäjäkunnan muuttuessa. Lisäksi pääsynhallinnan toiminnallisuuden tulee olla selkeästi kuvattu ja dokumentoitu, jotta toteutuksen arvioiminen ja koko prosessin auditoiminen olisi mahdollista. Pääsynhallinnan huolellinen suunnittelu paitsi takaa tietoturvallisen tavan hallita käyttäjien käyttöoikeuksia, myös nopeuttaa käyttöoikeuksien hakemiseen ja jakamiseen kuluvia toimenpiteitä, vähentää manuaalisen työn määrää, ja näin pienentää koko yrityksen operatiivisia kustannuksia.

Esitelty toteutusehdotus pyrkii esittelemään kattavan kokonaiskuvan siitä, miten pääsynhallinta voitaisiin toteuttaa IT-ulkoistuspalveluita tarjoavassa yrityksessä. Toteutusehdotuksessa on otettu huomioon erityisesti tietoturvan takaaminen pääsynhallinnassa, ja pääsynhallinnan määritteleminen palvelutoiminnoksi. Toteutusehdotuksessa ei pyritä ratkaisemaan yksittäisten käyttöoikeuspyyntöjen mahdollisimman tehokasta toteuttamista, mutta esitellään roolipohjainen pääsynhallintamenetelmä, jolla yksittäisten käyttöoikeuspyyntöjen määrää voitaisiin vähentää huomattavasti. Lisäksi toteutusehdotus esittelee reunaehdot, mitä teknisiä vaatimuksia valitun työkalun tulisi toteuttaa ja miten ne voidaan saavuttaa. Arvioinnin perusteella toteutusehdotus on yrityksen kannalta suositeltava toteuttaa, sillä se tarjoaa paitsi tehokkaamman tavan toteuttaa pääsynhallintaa yrityksessä, mahdollistaa myös toimintatavan linjaamisen yleisten alan standardien mukaiseksi ja lisää osaltaan yrityksen tietoturvaa.

8.3 Kehitysehdotukset ja jatkotutkimus

Pääsynhallinnan toteuttaminen onnistuneesti IT-ulkoistuspalveluita tarjoavan yrityksen sisällä on jo sinällään iso haaste. Palveluiden myyminen asiakkaille on luonnollisesti osa IT-ulkoistuspalveluita tarjoavan yrityksen ydinliiketoimintaa, jolloin palveluiden suunnittelussa tulee myös arvioida niiden soveltuvuutta erilaisiin asiakastarpeisiin. Kehitysehdotuksena pääsynhallintaan liitetty identiteetinhallinta yrityksen ja sen asiakkaiden välillä voitaisiin toteuttaa luvussa 4.3 mainitun yhdistetyn identiteetin mallin mukaisesti, ja rakentaa asiakaskohtainen pääsynhallintaratkaisu tukemaan tätä mallia. Toteutuksessa tulee kuitenkin aina ottaa huomioon, että kuten luvussa 5.1 on mainittu, ei ole olemassa yhtä oikeaa pääsynhallintamenetelmää, vaan menetelmä tulee valita aina ympäristöön ja tietoturva- ja käytettävyysvaatimuksiin soveltuvaksi.

Käyttöoikeuspyyntöjen provisiointi vaatii usein tuotantotiimin osallistumisen oi-

keuksien toteutukseen. Oleellinen jatkotutkimuksen kohde yrityksen kannalta on provisioinnin tehokkuuden arviointi. Tehokkuuden arvioinnilla voidaan tunnistaa ne käyttöoikeuskohteet, jotka vaativat eniten aikaa toteutuksessa. Lisäksi tulisi arvioida se, paljonko työtä vaatii provisioinnin toteuttaminen suoraan kohdejärjestelmiin tai *Active Directoryyn*, ja tämän tiedon vertaaminen tuotantotiimin oikeuksiin kuluttamaan aikaan.

Pääsynhallintamenetelmän valinta voi olla yrityksille vaikeaa sen vuoksi, että eri menetelmien vaikutukset toteutuksen tehokkuuteen ja tietoturvaan eivät välttämättä ole tiedossa etukäteen tai ovat vaikeasti ennustettavia. Jatkotutkimus eri pääsynhallintamenetelmien vaikutuksista tehokkuuteen ja tietoturvaan auttaisi yrityksiä vertailemaan menetelmiä keskenään paremmin. Lisäksi mahdollisuus käyttää useampaa menetelmää samanaikaisesti voi tuoda sellaisia etuja, joita ei yhdellä menetelmällä saavuteta.

Viitteet

[1] Office of Government Commerce. *ITIL Service Operations.* United Kingdom, The Stationery Office, 2007. ISBN 978-0-11-331046-3.

[2] Office of Government Commerce. *ITIL Service Design.* United Kingdom, The Stationery Office, 2007. ISBN 978-0-11-331047-0.

[3] Johansson, M. BS 7799, Tietoturvan Hallinta. Suomi, Helsingin Yliopisto, 2003.

[4] International Organization for Standardization. *ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management.* Switzerland, 2007-07-01.

[5] International Organization for Standardization. *ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements.* Switzerland, 2005-10-15.

[6] White, Gregory B., Fisch, Eric A. ja Pooch, Udo W. *Computer System and Network Security.* CRC Press, 1996. ISBN: 0-8493-7179-1.

[7] Johnston, R., Clark, C. *Service Operations Management - Improving Service Delivery.* Third Edition. Edinburgh Gate Harlow, Pearson Education Limited, 2008. ISBN 978-14058-4732-2.

[8] Macfarlane, I., Rudd, C. *itSMF The IT Service Management Forum: IT Palvelunhallinta – ITIL Käsikirja.* ISBN 0-9551245-2-2.

[9] International Organization for Standardization. *ISO/IEC 20000-1:2005 Information technology – Service management - Part 1: Specification.* Switzerland, 2005-12-15.

[10] Benantar, M. *Access Control Systems - Security, Identity Management and Trust Models.* United States of America, Springer Science+Business Media, Inc., 2006. ISBN 978-0-387-00445-7.

[11] Altmann, J., Sampath, R. UNIQuE: A User-Centric Framework for Network Identity Management. South Korea, Seoul National University.

[12] URI Planning Interest Group. URIs, URLs, and URNs: Clarifications and Recommendations 1.0. Verkkodokumentti. W3C/IETF. Viitattu 16.8.2011. Saatavissa: http://www.w3.org/TR/uri-clarification/.

[13] XDI.ORG. Infrastructure for accountable networks. Verkkosivu. XDI.ORG - an international non-profit public trust organization governing open public XRI and XDI infrastructure. Viitattu 16.8.2011. Saatavissa: http://www.xdi.org/.

[14] ISO. Management and leadership standards - Certification. Verkkodokumentti. International Organization for Standardization. Viitattu 29.8.2011. Saatavissa: http://www.iso.org/iso/iso_catalogue/management_and_leadership_standards/certification.htm.

[15] IsecT Ltd. ISO/IEC 2001 certification standard. Verkkodokumentti. IsecT infosec consulting. Viitattu 29.8.2011. Saatavissa: http://www.iso27001security.com/html/27001.html.

[16] Sandhu, Ravi S., Smarati, Pierangela. Access Control: Principles and Practice. *IEEE Communications Magazine,* September 1994.

[17] Jäntti, M., Lahtela, A., Kaukola, J. Establishing a Measurement System for IT Service Management Processes: A Case Study. *International Journal on Advances in Systems and Measurements,* 2010, vol. 3 no. 3 amd 4.

[18] European Committee for Standardization. *DIN EN ISO 9001:2008 Quality management systems – Requirements.* German, 2008.

[19] Inspecta. Sertifiointi. Verkkosivu. Inspecta Group, 2011. Viitattu 6.9.2011. Saatavissa: http://www.inspecta.com/fi/Palvelut/Sertifiointi/.

[20] Lampson, B. W. Protection. *ACM Operating System Review,* 1974, vol. 8, no. 1, s. 18-24.

[21] Bell, D. E. ja LaPadula, L. J. Secure Computer Systems: Mathematical Foundations. *MITRE Technical Report 2547,* 1973, vol. 1. Mitre Corporation, Bedford, MA, 1975.

[22] Ferraiolo, David F., Kuhn, R. Role-Based Access Controls. *15th National Computer Security Conference,* 1992, s.554 - 563. National Institute of Standards and Technology, USA, Gaithersburg, U.S. Department of Commerce, Md. 20899.

[23] Northcutt, S. Role Based Access Control to Achieve Defense in Depth. Verkkodokumentti. SANS Technology Institute, 2007. Viitattu 28.9.2011. Saatavissa: http://www.sans.edu/research/security-laboratory/article/311

[24] Mayfield, T., Roskos, J. E., Welke, S. R., Boone, J. M. Integrity in Automated Information Systems. *C TECHNICAL REPORT 79-91,* September 1991, National Computer Security Center (NCSC). Alexandria, Virginia.

[25] Vanamali, S. Role Engineering: The Cornerstone of Role-Based Access Control. *White Paper: Role Engineering and Role-Based Access Control.* CISA, CISSP. CA Services, July 2008.

[26] Coyne, Edward J. Role Engineering and Why We Need It. *Role Engineering for Enterprise Security Management,* 2007, Chapter 4. Artech House Publishers. ISBN: 9781607832225.

[27] Vaidya, J., Atluri, V., Guo, Q. The Role Mining Problem: Finding a Minimal Descriptive Set of Roles. *SACMAT–07,* 2007, June 20-22. Sophia Antipolis, France.

[28] Josang, A., Pope, S. User Centric Identity Management. CRC for Enterprise Distributed Systems and Technology (DSTC Pty Ltd), The University of Queensland, 4072, Australia. AusCERT Conference 2005.

[29] Gaedke, M., Meinecke, J., Nussbaumer, M. A Modeling Approach to Federated Identity and Access Management. University of Karlsruhe 2005.

[30] Kasanen, Hannu. Keskitetty identiteetinhallinta, Referenssiarkkitehtuuri. Secproof, Finland, 09/2010.

[31] Massachusetts Institute of Technology, Secure Endpoints Inc. Network Identity Manager 1.3.1. *User Documentation,* MIT Kerberos for Windows Release 3.2.2. Massachusetts Institute of Technology 2007.

[32] Microsoft. Active Directory Overview. Verkkodokumentti. Microsoft 2011. Viitattu 28.9.2011. Saatavissa: http://www.microsoft.com/en-us/server-cloud/windows-server/active-directory-overview.aspx.

[33] kansanvalta.fi. Koulutus ja kehittäminen. Verkkodokumentti. Kansanvalta.fi 2011. Viitattu 28.9.2011. Saatavissa: http://www.kansanvalta.fi/Etusivu/Tutkimusjakehitys/Sosiaalisenmedianmahdollisuudethallinnollepa/Koulutusjakehittaminen.

[34] Atos. Identity and Access Management with DirX. Verkkosivu. Atos 2011. Viitattu 29.9.2011. Saatavissa: http://atos.net/en-us/solutions/identity-security-and-risk-management/identity-and-access-management-with-dirx/default.htm.

A Roolitietojen keräämiseen käytetty kaavake

Team permissions

Template is filled with example information; please overwrite them with information relevant to the team.

Org. Unit: *FI UNIX*

E-mail groups:			
AD group membership	Target		Channel/Contact
Windows Server	*Team members*		*Approval from Superior and e-mail to service desk.*

Sharepoint:			
SharePoint Access Level	Target		Channel/Contact
Windows Server	*Team members*		*Lotus Notes Check In Request SharePoint Request*

Remote servers:			
Server	Target	Permission	Channel/Contact
Servername	*Team members*	*user*	*Superior requests through ARAP*

OSD:			
Profile	Target		Channel/Contact
Production	*Team members*		*Superior fills: OSD user account request form*

Clearances:			
Clearance	Target		Channel/Contact
DC1	*Team members*		*ARAP*

Portals:			
Portal	Target	Permission	Channel/Contact
CMWeb	*Team members*	*user*	*ARAP*

Notes:			
Tool	Target		Channel/Contact
ID	*Team members*		*Service Desk*

CATS:			
Project	Target		Channel/Contact
	Team members		*Project owner defines the organization units that can book hours to that project.*

B Vaatimusmäärittely pääsynhallinnan toteutusehdotukselle

Taulukko 11: Toteutusehdotuksen vaatimusmäärittely

Nro.	Nimi	Kuvaus	Prioriteetti
1	Käyttäjäystävällinen käyttöoikeuspyynnöille tarkoitettu käyttöliittymä	Käyttöoikeuspyyntöjen tekeminen onnistuu ilman ohjeistusta ja avustusta.	P
2	RBAC mallin käyttö.	Ratkaisu tukee RBAC mallia. Rooliperustainen pääsynhallinta vähentää yksittäisten pyyntöjen määrää ja selkeyttää pääsynhallintaa.	P
3	Sääntöihin perustuva automaattinen oikeuksien jakaminen.	Ratkaisu mahdollistaa sääntöihin perustuvan oikeuksien automaattisen jakamisen.	P
4	Käyttöoikeuskohteiden parannettu ylläpito ja hallinta.	Käyttöoikeuskohteet ovat ajan tasalla ja niiden ylläpito ja hallinta on helppoa.	P
5	Automaattinen pyynnön oikeellisuuden tarkistus.	Ratkaisu automaattisesti tarkistaa pyynnön oikeellisuus; saako hakija hakea oikeuksia, onko pyydetyt oikeudet jo olemassa, jne.	P
6	Automaattinen hyväksyjien määrittäminen	Ratkaisun tulee automaattisesti määrittää pyynnölle oikeat hyväksyjät, noudattaen SoD:ia.	P
7	Käyttöoikeuspyyntöjen provisioint tiketöintityökaluun.	Ratkaisu tukee pyyntöjen lähetystä tiketöintityökaluun toteutettavaksi tuotantotiimeille.	P
8	Automaattinen käyttöoikeuskohteiden jaottelu valittuihin kategorioihin.	Ratkaisu kykenee lajittelemaan pyydetyt oikeudet oikeisiin kategorioihin, jotta ne voidaan ohjata oikeaan tuotantotiimiin toteutettavaksi tiketöintityökalulla.	T

9	Tiketöintityökalun paluuviestien/statustietojen tulkitseminen.	Ratkaisu kykenee tulkitsemaan tiketöintityökalusta saatuja paluuviestejä ja muuttamaan käyttöoikeuspyynnön toteutuksen tilaa niiden mukaan.	P
10	Käyttöoikeuspyyntöjen provisiointi sähköpostiviestinä.	Ratkaisu tukee pyyntöjen lähetystä sähköpostiviesteinä toteutettavaksi valituille kohteille.	P
11	Käyttöoikeuspyyntöjen provisiointi suoraan kohdejärjestelmiin.	Ratkaisu mahdollistaa oikeuksien provisiointia suoraan kohdejärjestelmiin.	T
12	Automaattinen tilatietojen ilmoittaminen oikeuden pyytäjälle ja oikeuden saajalle.	Ratkaisun kykenee viestimään oikeuden pyytäjälle ja oikeuden saajalle toteutuneet ja hylätyt pyynnöt.	P
13	Omien käyttöoikeuksien tarkastelu käyttäjille.	Ratkaisu mahdollistaa käyttäjien tarkastella omia käyttöoikeuksiaan.	T
14	Pääkäyttäjille näkyvyys ja muokkausmahdollisuudet järjestelmiin joita he hallitsevat.	Ratkaisu mahdollistaa pääkäyttäjien tarkastella ja muokata hallinnoimiensa järjestelmien käyttöoikeuksia.	T
15	Kaikkien käyttöoikeuskohteiden hallinnoiminen.	Ratkaisu mahdollistaa kaikkien käyttöoikeuskohteisiin tehtyjen oikeuspyyntöjen hallinnoimisen riippumatta niiden luonteesta.	A
16	Käyttöoikeuskohteiden ja roolien etsiminen.	Ratkaisu mahdollistaa helpon tavan etsiä haettavia käyttöoikeuskohteita ja rooleja.	T
17	Usean käyttöoikeuskohteen hakeminen kerralla.	Ratkaisu mahdollistaa usean käyttöoikeuskohteen hakemisen käyttäjälle kerralla.	T
18	Oikeuksien hakeminen joukolle henkilöitä.	Ratkaisu mahdollistaa oikeuksien hakemisen usealle henkilölle kerralla.	A
19	Vanhentuneiden käyttäjätilien ja käyttöoikeuksien automaattinen poistaminen.	Ratkaisu mahdollistaa automaattisen vanhentuneiden käyttäjätilien ja käyttöoikeuksien poistamisen.	P
20	Käyttöoikeuspyyntöjen tilatietojen ja jaettujen käyttöoikeuksien tarkastelu.	Ratkaisu mahdollistaa pyyntöjen tilatietojen tarkastelun ja jaettujen käyttöoikeuksien listaamisen.	P